
# *ForeView*™ 4.2
# *ForeView RMON ST*
# User's Manual

MANU0169-01 -Rev A - April, 1997

Software Version 4.1.3

**FORE Systems, Inc.**

1000 FORE Drive
Warrendale, PA 15086
Phone: 412-742-4444
FAX: 412-772-6500
http://www.fore.com

## *Legal Notices*



## *TRADEMARKS*

# Table of Contents

# PART 1

# Using *ForeView RMON **ST*** With FORE Systems' LAN Switches

This part describes the *ForeView RMON **ST*** software and how to use it with the mini-RMON applications that are embedded in certain models of FORE Systems' LAN Switches. The three FORE Systems' LAN Switches that have embedded mini-RMON groups are as follows:

- PowerHub 7000
- PowerHub 6000
- *ForeRunner*™ ES-3810

The three models are collectively referred to in this manual as FORE Systems' LAN switches.

In addition to mini-RMON, the *ForeRunner* ES-3810 has Roving RMON embedded, and any sections dealing with Roving RMON apply to the *ForeRunner* ES-3810.

This part contains the following chapters:

# CHAPTER 1 About This Manual

## 1.1 Who Should Read This Manual

The information in this manual is designed to help you monitor traffic and diagnose emerging problems on network segments using *ForeView RMON **ST*** and *ForeView* Expert Visualizer.

Guidelines for installing the *ForeView RMON **ST*** and *ForeView* Expert Visualizer software are included, as well as basic information you might want to review before getting into advanced procedures. You'll use various information provided here depending on your needs. This manual is best used as a reference, and after reading Chapter 2 for installation instructions and Chapter 3 for a basic undertanding of the software, we recommend using the index and this chapter to determine which sections you need to read.

This chapter outlines the information contained in this book and indicates the major tasks that are covered. For information about other *ForeView RMON **ST*** products and supplementary information that might be useful, see Related Documentation on page 1-6.




Before installing and running *ForeView RMON **ST***, you should be familiar with your Operating System (Motif or Solaris), and your Sun SPARC, HP 9000, or IBM RS6000 platform. See Chapter 2 for system requirements and installation instructions.

## 1.2 Chapter Summaries

This *ForeView RMON **ST** User's Guide* contains information you need to work with all of the *ForeView RMON **ST*** applications and tools. The book includes basic and advanced procedures for monitoring and viewing network segment traffic, as well as extensive information about logging and reporting the statistics collected. The book contains three parts:

- Part 1 (Chapters 1 through 11) contains information on using *ForeView RMON **ST*** with agents embedded in FORE Systems' LAN Switches
- Part 2 (Chapters 12 through 16) contains information on using *ForeView RMON **ST*** with network probes
- Part 3 contains the Appendices.

The following topics are covered in the *ForeView RMON **ST*** User's Manual:

- **CHAPTER 1: About This Manual** — Tells you how this book is organized, describes the conventions, notation, and symbols used in this book; tells you how to get help from FORE Systems, and lists other related documentation.
- **CHAPTER 2: Installing *ForeView RMON ST*** — Tells you how to install *ForeView RMON **ST*** Manager. Installation instructions include recommended system requirements and step-by-step installation procedures. Chapter 2 also tells you how to install the *ForeView* Expert Visualizer software. For more information on *ForeView* Expert Visualizer, see the *ForeView Expert Visualizer User's Guide.*
- **CHAPTER 3: Learning *ForeView RMON ST* Basics** — Tells you how to start *ForeView RMON **ST*** Manager and describes the *ForeView RMON **ST*** Manager main window. You should read this chapter even if you have a solid background in network management because it explains features that are exclusive to *ForeView RMON **ST*** Manager products.
- **CHAPTER 4: Working with Agents, Groups, and Switches** — Tells you how to add agents, agent groups, or switches to *ForeView RMON **ST*** Manager for network monitoring and troubleshooting.
- **CHAPTER 5: Monitoring the Network using Traffic Monitor** — Tells you how to perform monitoring and troubleshooting at the physical network layer. Also describes the three different Traffic Monitor modes you can run.
- **CHAPTER 6: Working with Domains and Domain Manager** — Tells you how to install and deinstall domains on an agent, and how to monitor domains using Domain Manager.
- **CHAPTER 7: Monitoring and Troubleshooting Single Domains —** Tells you how to look at traffic for a single domain.
- **CHAPTER 8: Setting Alarms Using Trap Manager —** Tells you how to monitor data thresholds by setting traps.
- **CHAPTER 9: Logging and Reporting with Trend Reporter —** Tells you how to use SQL queries to generate custom reports from the command line. Describes various database tables and daemons you'll use to do so. Also covers information about administering the database.
- **CHAPTER 10: Customizing Trend Reporter —** Tells you how to use Trend Reporter's GUI to generate reports interactively. Both interactive and command-line reports are available.
- **CHAPTER 11: Decoding Captured Packets with Protocol Decode —** Tells you how to capture selected data and examine single packets. Raw Hex mode and Full Frame Decode functions are included.

- **CHAPTER 12: *ForeView RMON ST* and Network Probes —** Gives you a brief overview of the Mini-RMON, Roving RMON, and Proxy RMON capabilities supported by *ForeView RMON* ***ST*** Manager.
- **CHAPTER 13: *ForeView RMON ST* Domains and Network Probes —** Covers RMON Domains as used by *ForeView RMON* ***ST*** in different RMON ***ST*** applications. This chapter also includes other information that applies specifically to network probes.
- **CHAPTER 14: Monitoring Token Ring Networks** — Tells you how to monitor statistics specific to Token Ring networks.
- **CHAPTER 15: Monitoring FDDI Networks with Ring Monitor** — Tells you how to monitor statistics specific to FDDI networks.
- **CHAPTER 16: Customizing Filters and Domains** — Tells you how to create your own customized filters for data capture and domain creation. Also tells you how to create your own customized domains.
- **APPENDIX A: Startup and Configuration Files** — Describes these files.
- **APPENDIX B: Error Messages** — Provides a list of common error messages.
- **APPENDIX C: Assigned Numbers** — Describes how to get a copy of RFC 1700, which lists and describes the "well-known" port names and numbers.
- **APPENDIX D: NETscout Probe Applications** — Tells you how to manage network resources both locally and remotely with Resource Monitor.

# 1.3 Document Conventions

This section describes and illustrates the conventions used in the book. You should become familiar with the document conventions before you begin working with the manual.

## 1.3.1 Typographical Conventions

The following typographical conventions are used in this manual.

| When you see this: | It means this: | For example: |
|---|---|---|
| Commands in **bold** and on a separate line. | Specific commands to be entered by the user. | **cd $FVHOME/usr** |
| Commands, Menu selections, such as File/Run, or file names that appear within text of this manual. | Words used as commands, menu selections or file names. | ...see the atmarp command for info.<br>...and more about the x.swp file... |
| Words within the less-than and greater-than symbols. | Words representing function keys on the keyboard. | Press <Enter>. |
| Words shown in **bold**. | Field names, list box names, and section names within a window; also used for emphasis. | Select an agent from the **Agents** list box...<br>...type the printer name in the **Printer** field. |
| Words shown in **bold** within the less-than and greater-than symbols (**< >**). | Provide a filename, path, or system variable; however, do **not** type the symbols. | Specify the **<install_path>** created in step 2... |
| Words shown in a monospaced font. | Messages or information that appears on the computer screen. | The message "`Learning ports for switch1...`" is displayed. |

## 1.3.2 Important Information Indicators

Text notes are always called out by one of the following three textual markers: Note, Caution, or Warning. When you see these markers, explained below, you'll know what kind of information to expect from the related text notes.


This is the Note text note. The note text provides information and reminders relevant to the successful operation of the system hardware and software.

**CAUTION**

This is the Caution text note. A caution text note provides information you need to know to prevent operations problems with system hardware or software.

***WARNING!***

This is the Warning text note. A warning text note provides **extremely important** information you **must** read to prevent damage to the system hardware or to the person operating the hardware.

## 1.3.3 Procedures

Procedures begin with a feature description, followed by step-by-step, numbered instructions. When procedures require you to supply user-defined information, refer to the table on page 1-4.

The following paragraphs show how procedures are displayed.

1. Numbered steps tell you what action to take and the order in which the steps should be performed.
2. Numbered steps may give you options, as shown below:
   - Option 1 and criteria required.
     *or*
   - Option 2 and criteria required.

## 1.4 Technical Support

In the U.S.A., you can contact the FORE Systems TAC (Technical Assistance Center) by any one of the following four methods:

1. If you have access to the Internet, you may Contact the FORE Systems TAC via email at the following Internet address:

   **info@fore.com**

2. You may access the FORE Systems Web Page at:

   **http://www.fore.com**

3. You may send questions via U.S. mail to the following address:

   **FORE Systems**

   **1000 FORE Drive**

   **Warrendale, PA 15086**

4. You may telephone your questions for support to:

   **1-800-671-FORE**

Non U.S. customers can get support through their local distributors.

When contacting the FORE Systems TAC, please be prepared to provide information such as your support contract license number, the serial numbers of your products, and as much information as possible describing your system configuration and your problem or question.

## 1.5 Related Documentation

*ForeView™ Expert Visualizer User's Guide*

If you choose to install the *ForeView* Expert Visualizer application when you install *ForeView RMON* ***ST***, refer to the *ForeView Expert Visualizer User's Guide* for more information on the Expert Visualizer application.

# CHAPTER 2 Installing *ForeView RMON ST*

This chapter tells you how to install the *ForeView RMON* ***ST*** and *ForeView* Expert Visualizer software. This chapter includes the following:

- An overview of the installation procedure.
- Hardware and software configuration requirements.
- Instructions for installing the software.




If you have installed *ForeView RMON* ***ST*** and *ForeView* Expert Visualizer as part of *ForeView* 4.2, then skip this chapter and go to CHAPTER 3: Learning ForeView RMON ST Basics.

## 2.1 Installation Guidelines

The following installation guidelines are designed to guide you through the installation of *ForeView RMON* ***ST.*** Read through this section before you start the installation.

The following list provides information about what you need before, during, and after the installation.

- Before installation:
  - Make sure that you've already installed the required hardware, software and network configuration. The table shown in the Section 2.1.1 on page 2-2 lists the supported configurations.
  - Make sure that you know the root password of the system on which you are installing *ForeView RMON* ***ST***.
  - If you are using third party probes, connect each probe to the network using the installation procedures described in the documentation that accompanied the probe(s).
- During Installation:
  - Install the *ForeView RMON* ***ST*** software by running the Install script. The installation will allow you to install *ForeView RMON* ***ST*** on its own, or both *ForeView RMON* ***ST*** and *ForeView* Expert Visualizer.

- After Installation:
  - Perform any appropriate network diagnostics to ensure that your network and the RMON agents on the switches or on the network probes are functioning properly.

### 2.1.1 System and Software Configuration Requirements

The following table lists the hardware and software configurations supported by *ForeView RMON* ***ST.*** If your configuration does *not* match one of those listed below, call the FORE Systems TAC (Technical Assistance Center) for information.

| **The following configurations support *ForeView RMON* ST:** |
|---|
| • Sun SPARC station or compatible<br>• Solaris 2.3 or higher<br>• OpenWindows 3.3 (SunOS Patch #100444-x must be applied when using without Motif)<br>*or*<br>• Motif Window Manager (GUI applications are statically linked with Motif 1.2.4 and X11R5 libraries)<br>• 48 MB RAM<br>• 80 MB minimum free disk space<br>• CD-ROM drive |
| • HP 9000 series 700<br>• HP/UX v 9.9 and higher<br>• Motif 1.2 and X11R5 libraries (included with HP-UX)<br>• 48 MB RAM<br>• 40 MB minimum free disk space<br>• CD-ROM drive |
| • IBM RS/6000<br>• AIX Version 3.2.4 and higher<br>• Motif 1.2.4 and X11R5 libraries<br>• 48 MB RAM<br>• 40 MB minimum free disk space<br>• CD-ROM drive |

# 2.2 Installing *ForeView RMON ST* Software

This section describes the steps needed to install *ForeView RMON **ST*** and *ForeView* Expert Visualizer.

## 2.2.1 Installing *ForeView RMON ST*

To install FORE Systems' *ForeView RMON **ST*** software onto a system, do the following:

1. Login as root user.
2. Insert the *ForeView* 4.2 CD in the CD-ROM drive and mount the file system as /cdrom, using the appropriate device name and mount command for your OS. See the documentation for your OS for more information.
3. Switch to the UNIX directory on the CD-ROM by typing the following:

   **cd /cdrom/unix**

4. Launch the installation script by typing the following command:

   **./install**

5. Follow the directions in the install script to install *ForeView RMON **ST*** and *ForeView* Expert Visualizer.

After the installation is complete, start *ForeView RMON **ST*** by changing to the /usr/fore/foreview/bin directory and typing the following command.

**./fvrmon**

# CHAPTER 3 Learning *ForeView RMON ST* Basics

*ForeView RMON* ***ST*** is a software package that lets you monitor, troubleshoot, and record information about your network's operation. Using *ForeView RMON* ***ST***, you can identify and isolate a wide variety of fault conditions in data communications networks.

*ForeView RMON* ***ST*** is based on the following standards, which allow it to operate in a multi-topology, multi-vendor environment:

- The **Simple Network Management Protocol (SNMP)**, which defines the protocol for all intercommunications between *ForeView RMON* ***ST*** and FORE Systems' LAN Switches, and between *ForeView RMON* ***ST*** and external probes.
- The **Remote Monitoring Management Information Base (RMON-MIB)**, which defines the type of information that the agent gathers that's available for you to display for each network segment.



This chapter describes *ForeView RMON* ***ST*** and how to use it. This chapter is divided into the following sections:

## 3.1 How *ForeView RMON ST* Works

*ForeView RMON **ST*** is a set of software application programs that you use as a starting point to issue operational commands to RMON agents to gather and analyze network information. *ForeView RMON **ST*** displays all results and diagnostic information. You can have multiple *ForeView RMON **ST*** programs active simultaneously within a single network, even working with the same RMON agent.

*ForeView RMON **ST*** works as a distributed system by using a central management console running the software in conjunction with data-gathering agents located at various points on a network. It can simultaneously collect wide-ranging statistical data, display selectively captured and fully decoded network traffic, set user-defined alarm conditions, and get real-time updates from all segments of a widely dispersed internetwork. *ForeView RMON **ST*** does all this from a centralized, SNMP-compatible network management console.

## 3.2 *ForeView RMON ST* Features

*ForeView RMON **ST*** has four main features:

- Monitors network traffic and measures the flow of data.
- Captures network traffic and records it for later examination (*ForeRunner* ES-3810 only).
- Interprets raw network data and translates it into a graphic form that you can view and analyze.
- Sets limit conditions on network traffic and generates alarms if those limits are exceeded.

*ForeView RMON **ST*** gathers and analyzes network information using RMON agents attached to network segments. It also can analyze data collected by third-party network probes.

You use these features by launching applications from the main window, then using tools to focus on detailed information.

Applications are launched by either clicking on an icon displayed in *ForeView RMON **ST*** main window, or by selecting Application from the menu bar and then choosing the application you want.

## 3.3 Starting *ForeView RMON* ST

After you've *completely installed* the *ForeView RMON* ***ST*** software, you're ready to get started. To start *ForeView RMON* ***ST***, use the following procedure.

1. From the UNIX command line, make the *ForeView RMON* ***ST*** installation directory your current directory:

   **cd usr/fore/foreview/bin**

2. Type the following command:

   **./fvrmon**


You must have root permission to run *ForeView RMON* ***ST***.



## 3.4 The *ForeView RMON* ST Main Window

*ForeView RMON* ***ST*** is a collection of applications that you can launch to monitor and manage your network.

After you start *ForeView RMON* ***ST***, the main window (see Figure 3.1 on page 3-4) is displayed.

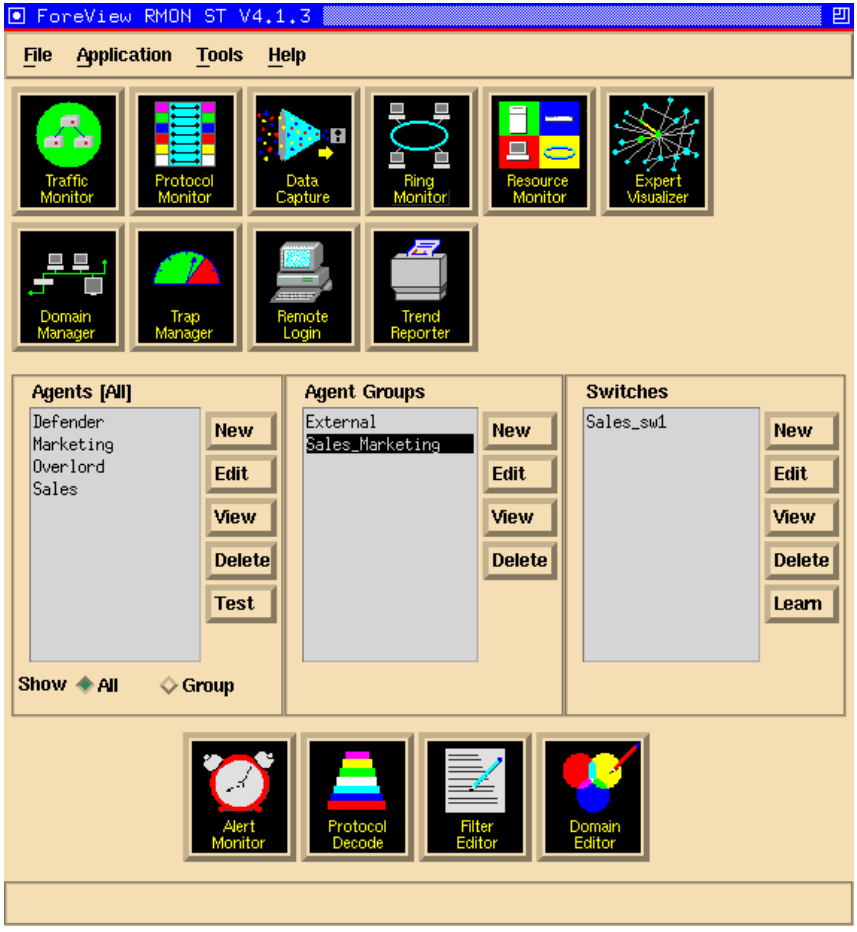



**Figure 3.1 -** *ForeView RMON* ***ST*** main window.

The icons in the top portion of the window let you open a *ForeView RMON* ***ST*** application. The application you open gathers information using the agents, agent groups, or switches you have selected from the selection boxes in the middle of the window. The **Agents [All]** list box, which contains the names of individual agents and selection buttons associated with those agents, is displayed on the left side of the main window. A similar list box, **Agent Groups**, is displayed in the middle of the window, and contains all the defined groups of agents. The **Switches** list box displays any switches that have been configured. When you first start *ForeView RMON* ***ST***, the **Agents [All], Agent Groups** and **Switches** list boxes are empty. The icons at the bottom of the window let you fine tune an application.

The *ForeView RMON* ***ST*** main window contains the applications listed in Table 3.1.

The columns to the right of the application descriptions indicate whether you need to select an agent, group, or switch before opening the application. The final column indicates the products with which you can use the application. "All" indicates you can use the application with FORE Systems' LAN Switches as well as with other vendors' products. "ES-3810" indicates the application is supported on the *ForeRunner* ES-3810 but not on the other FORE Systems' LAN Switches. "Probe" indicates that the application is not supported on the FORE Systems' LAN Switches, but instead requires that you install a NETscout Probe.

**Table 3.1 -** *ForeView RMON* ***ST*** Applications

| Application | Single or Multiple Agents | Single Agents Only | No Agent Selection Required | Switch Support |
|---|---|---|---|---|
| **Traffic Monitor**<br>Lets you graphically monitor MAC-layer statistics for multiple network segments.<br>You can use Traffic Monitor to establish a baseline of "normal" or expected performance and note any deviations from that performance that might signal broader network problems. You can then launch additional *ForeView RMON* ***ST*** tools to examine these suspect areas, or simply monitor certain aspects of your network in greater detail. | X | | | All |
| **Protocol Monitor**<br>Gives you an overview of network activity by converting raw network data gathered by agents and switches into easy-to-read graphical displays—displays you can transpose and invert to get two different views of the same data. Graphically displays network traffic statistics simultaneously for a number of selected agents, providing at-a-glance comparison of multiple network segments. | X | | | Probe |
| **Data Capture**<br>Captures packets selectively from an RMON agent and saves them in a file. After you capture packets, you can examine them using Protocol Decode. | X | | | ES-3810 |

**Table 3.1 -** *(Continued) ForeView RMON* ***ST*** Applications

| Application | Single or Multiple Agents | Single Agents Only | No Agent Selection Required | Switch Support |
|---|---|---|---|---|
| **Ring Monitor**<br>Lets you examine your FDDI network. Ring Monitor builds a ring map by collecting SMT Neighbor Information Frames (SMT-NIFs). | X | | | Probe |
| **Resource Monitor**<br>Enables the use of proxy resources to lessen the demands placed on resources by RMON activities. | | X | | Probe |
| **Expert Visualizer**<br>Gives you a graphical view of your network. Expert Visualizer gives you the ability to see a large number of agents and devices in your network and then focus on problem areas using the other *ForeView RMON* ***ST*** applications. | X | | | All |
| **Domain Manager**<br>Lets you assign agents to segments or ports on a switch using the mini-RMON and Roving RMON groups embedded in the FORE Systems' LAN switches. *ForeView RMON* ***ST*** polls the agent for Ethernet statistics and history statistics, and lets you set traps that will set off alarms. | X | | | All |
| **Trap Manager**<br>Lets you monitor your network, and specific network devices, by setting alarms on selected events associated with any RMON-MIB variable. You can perform such monitoring when you suspect a fault in the segment or device, or just to be notified if it develops problems. | X | | | All |
| **Remote Login**<br>Lets you configure a NETscout Probe. Remote Login is not supported on the FORE Systems' LAN Switches. | | X | | Probe |

**Table 3.1 -** *(Continued) ForeView RMON* ***ST*** Applications

| Application | Single or Multiple Agents | Single Agents Only | No Agent Selection Required | Switch Support |
|---|---|---|---|---|
| **Trend Reporter**<br>Enables you to log and report statistics related to your network. Trend Reporter is based on a relational database, which means that you can make ad hoc queries to information contained in any of the database's tables, set up automatic report generation, choose reports based on detail or summary data, and define how long detail or summary information stays in the database. Trend Reporter includes a bundled Structured Query Language (SQL) server. | X | | | All |
| **Alert Monitor**<br>Displays information about traps you define using Trap Manager. Alert Monitor flashes you to indicate receipt of a trap message and displays the alert messages. | | | X | All |
| **Protocol Decode**<br>Lets you examine previously-captured data packets that are stored in a file that you define. | | | X | ES-3810 |
| **Filter Editor**<br>Lets you edit existing filters or create new filters to meet your requirements. | | | X | Probe |
| **Domain Editor**<br>Lets you create new domains or edit existing domains to meet your monitoring needs. You can choose to create generic or protocol-specific domains in *ForeView RMON* ***ST***. Also lists the available filters. | | | X | All |

### 3.4.1 Launching Applications

This section assumes that you are familiar with Agents, Groups, and Switches. This section also assumes that you understand the RMON support required by the *ForeView RMON **ST*** applications and the RMON support provided by FORE Systems' LAN Switches.

For information about Agents, Groups, and Switches, see ForeView RMON ST Concepts on page 3-11.

For information about RMON support, see RMON Support on page 3-11.

If you need help using the *ForeView RMON **ST*** windows, see ForeView RMON ST Window Conventions on page 3-14.

To launch an application from the *ForeView RMON **ST*** main window:

1. Select an Agent, Agent Group, or Switch. If no Agents, Groups, or Switches are available for selection, you need to add them. See Chapter 4: Working with Agents, Groups, and Switches.
2. Click on the application icon.
3. See the appropriate chapter in this manual for information about how to use the application.

**Table 3.2 -** *ForeView RMON **ST*** Application Information

| Application | See |
|---|---|
| **Traffic Monitor** | Monitoring the Network using Traffic Monitor on page 5-1 |
| **Protocol Monitor** | Using Protocol Monitor on page D-16 |
| **Data Capture** | Decoding Captured Packets with Protocol Decode on page 11-1 |
| **Ring Monitor** | Monitoring Token Ring Networks on page 14-1<br>or<br>Monitoring FDDI Networks with Ring Monitor on page 15-1 |
| **Resource Monitor** | Managing Remote Resources with Resource Monitor on page D-2 |
| **Expert Visualizer** | The *Expert Visualizer User's Guide* |
| **Domain Manager** | Working with Domains and Domain Manager on page 6-1 |

**Table 3.2 -** *(Continued)* *ForeView RMON* ***ST*** Application Information

| Application | See |
|---|---|
| **Trap Manager** | Setting Alarms Using Trap Manager on page 8-1 |
| **Remote Login** | Remote Login on page D-26 |
| **Trend Reporter** | Logging and Reporting with Trend Reporter on page 9-1 |
| **Alert Monitor** | Viewing a List of Traps Using Alert Monitor on page 8-14 |
| **Protocol Decode** | Decoding Captured Data Using Protocol Decode on page 11-8 |
| **Filter Editor** | Customizing Filters and Domains on page 16-1 |
| **Domain Editor** | Defining New Domains on page 16-10 |



## 3.4.2 Launching Tools

After you launch a *ForeView RMON* ***ST*** application, you usually can then launch other tools that help you "drill down" to show more details. Also, you sometimes can choose yet other tools once you've drilled down. Most drill-down tools are available from applications that require you to select at least a single agent (although some tools are available when you use applications that let you monitor multiple agents). Tools that you can launch from single or multiple agent applications, as well as from other tools are as follows:

- Segment Statistics
- Segment History (short-term history and long-term history are available)
- Segment Zoom (tabular and graphical versions are available)
- Host List[1]
- Host Zoom (tabular and graphical versions are available)[1]
- Top N Hosts[1]
- Host History[1]
- Conversation History[1]
- Conversation List[1]

1. These tools are part of the RMON standard, but not part of the mini-RMON standard, They are supported by the *ForeRunner* ES-3810, but not the PowerHub 6000 or 7000 switches.

- Source Routing Monitor[1]

See the chapter that describes the application you are using for information about the tools you can use with that application.

## 3.5 Printing Graphs and Data

*ForeView RMON **ST*** lets you print most screens that contain graphs and numerical data. You can also print reports. To print graphical screens, you must have a postscript printer. To print numerical data, you can use any printer. Use the following procedure when you need to print something from *ForeView RMON **ST***.

1. Select **File/Print** from the menu bar. The Print Options dialog box appears as shown in Figure 3.2.


**Figure 3.2 -** Print Options Box

2. Do one of the following:
   - To print to a file, select **File** as the destination, specify the directory path under **Directory**, and type the filename in the **File** field.
     *or*
   - To print directly to a printer, select **Printer** as the destination, and type the printer name in the **Printer** field.
3. Click on **Apply**.

# 3.6 Exiting *ForeView RMON ST*

You can exit *ForeView RMON **ST*** at any time. When you do so, *ForeView RMON **ST*** saves all the changes you've made, such as adding agents, agent groups, or switches, and installing domains. To exit *ForeView RMON **ST***, select **File/Exit** from the main window menu bar.

# 3.7 *ForeView RMON ST* Concepts



## 3.7.1 Agents, Groups, and Switches

The terms agent, agent group, and switch have special meanings when you are using *ForeView RMON **ST*** to manage a PowerHub switch or *ForeRunner* ES-3810:

**Agent** — Software on the switch that is applied to a single segment on a PowerHub switch or *ForeRunner* ES-3810.

**Group** — A user-defined collection of agents on a PowerHub switch or *ForeRunner* ES-3810.

**Switch** — A FORE Systems' LAN Switch or other RMON supported switch. The switch must be selected and defined before agents can be attached to the switch's segments.

Before you click on an application icon to open the application, you add and select agents, agent groups, or switches. When you open an application, the application gathers and displays information for the agents, groups, or switches you have selected.

After you launch an application, you usually can then launch tools that help you "drill down" to show more details. When you open an application, consult the chapter in this manual that describes the application for information about the tools you can use with the application.

## 3.7.2 RMON Support

Whether an application can be used with a specific PowerHub switch, *ForeRunner* ES-3810, or other type of switch depends upon the RMON support in the switch and the RMON support required by the application. Some applications are designed for Roving RMON support, standard RMON support or proprietary MIB support.

The PowerHub 6000 and 7000 support the mini-RMON, but not standard RMON or Roving RMON. The *ForeRunner* ES-3810 supports mini-RMON, standard RMON, and Roving RMON.

Applications that cannot be used for the agent, agent group, or switch that you select are grayed out and therefore are unavailable for use.

### 3.7.2.1 The RMON-MIB Standard

The first standard for network management evolved into a specification that became known as SNMP (Simple Network Management Protocol). SNMP was given RFC number 1098 by the IETF (Internet Engineering Task Force). By embedding the basic SNMP MIB within data communication devices, multi-vendor management systems can manage these devices from a central site and view information graphically.

The basic MIBs used with SNMP have limitations. Although MIBs allow regular polling of devices, they don't provide for extensive active monitoring of critical functions or monitoring network traffic on a LAN segment. Other SNMP-based network devices can identify only traffic specifically addressed to themselves and cannot provide statistics on conversations *between* devices—an important concept for network troubleshooting. RMON-MIB is designed to address many of these limitations.

RMON-MIB, (Remote MONitoring-Management Information Base) was developed by the IETF (Internet Engineering Task Force) and became a standard in 1992 as RFC number 1271. The RMON-MIB specification was developed to provide traffic statistics and analysis on many network parameters for comprehensive network fault diagnosis, planning, and performance tuning.

In 1994 RFC 1513 was added. RFC 1513 specifies characteristics associated with the token ring topology. RFC 1757 for Ethernet RMON was released in 1995, obsoleting RFC 1271.

RMON-MIB delivers seamless multi-vendor interoperability between SNMP management stations and monitoring agents. It also provides a standard for a set of MIBs which collect rich network statistical information not available from the standard SNMP MIB.

Finally, RMON-MIB allows active network diagnostics through a powerful Alarm Group that lets you set thresholds for critical network parameters, to automatically deliver alerts to centrally located management consoles.

### 3.7.2.2 Basic RMON Groups

This section describes the basic RMON-MIB groups. An RMON-MIB group is a related set of variables used with RMON functions, such as monitoring and collecting certain types of data, setting alarms, and event trapping. RMON goes far beyond SNMP in providing useful tools for network monitoring.

#### 3.7.2.2.1 Standard RMON-MIB Groups

The standard RMON-MIB groups for Ethernet networks are:

- Statistics
- History

- Alarms
- Host
- Host Top N
- Matrix
- Filters
- Packet Capture
- Events

#### 3.7.2.2.2 Mini-RMON Groups

Mini-RMON is a subset of the Standard RMON-MIB groups. Mini-RMON is embedded in FORE Systems' LAN Switches and includes the following subset of the standard RMON groups:

- Statistics
- History
- Events
- Alarms

#### 3.7.2.2.3 Roving RMON Groups

Roving RMON contains the same groups as the standard RMON MIB. In Standard RMON, groups can be assigned to monitor multiple segments simultaneously. In Roving RMON, groups that are not in the mini-RMON-MIB groups can be gathered from only one segment at a time. The RMON function "roves" to the segment from which information is requested. Statistics, History, Events, and alarms can be used globally on a switch, while Host, Host Top N, Matrix, Packet Capture, and Events groups "rove" to the specific segment from which information is requested.


While Roving RMON will work on any port on the *ForeRunner* ES-3810, it must be assigned to a port before it will begin to gather statistics. To "rove" to a new port, you must first remove roving from the current port and then assign it to the new one. This is done by assigning the Host and Conversation agents to the desired ports using Domain Manager. If you try to assign the Host and Conversation agents to a port when they have already been assigned to a different port, you will get the message: `Error: No resources in Agent.`

#### 3.7.2.2.4 RMON2 Support

RMON2 supports enhanced RMON functionality and is not included in the mini-RMON standard. RMON2 requires additional resources and bandwidth as a result of the increased functionality and the trade-off between the two is not always desirable. For more on the RMON2 standard, see Chapter 12: ForeView RMON ST and Network Probes.

### 3.7.3 Network Probes

RMON agents that are present on FORE Systems' LAN Switches can be attached to any segment connected to the hub. An alternative to using the mini-RMON and Roving RMON agents that are present on the FORE Systems' LAN Switches is using a network probe. Network probes are RMON probes that you attach to a specific network segment. The network probe gathers statistical information for that segment and provides a window into the segment which you use to observe and analyze network data, much like the RMON agents on the FORE Systems' LAN Switches. A typical network has multiple segments and multiple agents. Normally, one agent is attached to each network segment.

For more information about network probes, please contact FORE Systems TAC.

### 3.7.4 Domains

When you're working with *ForeView RMON **ST***, you'll see the term "domain" used often; in this document, this term is used to describe the kinds of traffic that you want to see statistics for. In other words, a domain lets you choose to display a specific traffic stream. Of the three network layers of traffic, MAC, Network, and Application, mini-RMON can monitor traffic on the MAC layer. For information on the Network and Application layers, see PART 2: Using ForeView RMON ST With External Network Probes.

The MAC layer includes basic RMON protocols that operate on the data link and physical layers. For example, *ForeView RMON **ST***'s RMON domain is a MAC-layer protocol.

The RMON domain is the only domain that can be used with the FORE Systems' LAN Switches; the other domains are proprietary and require a NETscout probe. The RMON domain, however, provides RMON statistics for *all* the traffic on the segment or switch, and can be configured to meet specific network monitoring needs.

## 3.8 *ForeView RMON ST* Window Conventions

Each application that appears in *ForeView RMON **ST*** runs in a **window**. Within some windows are **menus**, which provide lists of choices. Beneath menus on some windows are **selection buttons**. When you click on them, selection buttons either start a single action or give you another list of choices. Windows can also contain **displays**, where *ForeView RMON **ST*** dis-

plays graphical network data, and **list boxes**, which contain tabular data related to the window's function.

### 3.8.1 Mouse Conventions

You perform most mouse selection with the left mouse button. The terms **select** and **click** *or* **click on** refer to a single mouse click.

### 3.8.2 Entering Window Information

When you enter information into *ForeView RMON **ST*** windows, there are a few restrictions you'll have to keep in mind:

- All names (agents, filters, domains, and other nameable entities) *must* start with a letter.
- Names can contain *only* letters, numbers, dashes, and underscores.
- When naming agents, agent groups, switches, domains, and filters, you can use *up to* 15 characters. (Keep in mind that *all names* are case sensitive).
- All numeric data entries are decimal integers unless stated otherwise.

### 3.8.3 Using Multiple Windows

You can open multiple *ForeView RMON **ST*** tools at the same time. You can also open multiple windows of the same tool at once. When you do this, however, remember that each window has an independent sample rate (30 seconds, 1 minute, and so on), so updates can be different with different windows. Thus, you can be monitoring the same data with two versions of the same window, and the data may appear different.

Also remember that when you open multiple windows, you use extra network resources. It's good practice to open only the windows you need to do your work.

## 3.9 Terminology

This section describes terms common to standard communication networks as well as terms used in this manual.

## 3.9.1 Common Network Terms Used in this Manual

**IP address** The four-byte Internet Protocol address uniquely identifying each node on the network. SNMP uses IP addresses to identify nodes to query and manage. SNMP is the underlying protocol used for *ForeView RMON **ST*** communications. The IP address format is X.X.X.X, where X is an integer with a decimal value of 0 through 255.

**MIB** SNMP network devices store information about themselves in a Management Information Base (MIB) located within an agent. A MIB contains "managed objects" (variables) that describe the characteristics and current state of a network device. You can manage an SNMP device by querying or setting its MIB variables.

A standard or public MIB is one where definitions of the MIB variable have been approved by a standards organization (IETF) and published for general use. A private MIB is a vendor-specific proprietary MIB, typically designed to extend a standard MIB and to collect specific segment traffic unique to the vendor's network devices.

**Network** A group of interconnected nodes that can communicate with one another and that use the same network address.

When multiple network segments are connected, they form an **internetwork.** Data passes from network to network by devices such as bridges, routers, and gateways using individual network addresses.

**Node** An individually addressable location on a data communications network. In RMON-MIB terminology, Host and Node are identical. A node is a network connection in any of a variety of physical devices such as personal computers, larger scale server computers, printers, and so on. A physical device can have multiple connections to a network and therefore may comprise multiple nodes.

**Segment** A network or subnet in which all nodes are physically and logically connected in such a way that all nodes receive all data traffic seen by all other nodes on the segment.

This means a segment can be either a single physical bus or loop, or may be interconnected by repeaters that pass all traffic. A segment *cannot* be connected by bridges, routers, or gateways, because these devices logically separate networks.

## 3.9.2 *ForeView RMON ST* Terms Used in this Manual

**Agent** — An agent is software installed on a node attached to a specific network segment to gather statistical information for that segment. An agent can be included in a specialized hardware and software package, such as a NETscout Probe, that you connect to a network segment to monitor it. It can be software included in an existing network device, such as the embedded RMON agent found in FORE Systems' LAN Switches and many network devices. The agent includes the MIB that stores device information, and gives you a window into the network segment so you can see and analyze network data.

**Agent** (or **agents**) is also used as a term to collectively indicate that you can choose an agent, agent group, or ports on a switch.

**Agent Group** — An agent group is a user-defined collection of agents used to consolidate and organize information about the network.

**Switch** — A switch is a network device used to increase throughput and performance by microsegmenting the network. You can also use switches to segment networks into logically-defined workgroups, called Virtual LANs (VLANs).

**Domain** — A domain is a definable variable that can include one protocol or a group of protocols. It can also be used to define devices and applications. You would use a domain to see all traffic on a network segment that matches the protocol specified in the domain.

**Scope** — A user-defined set of agents and domains that *ForeView RMON **ST*** monitors.

**Conversation** — Conversation is *ForeView RMON **ST***'s term for the set of statistics (RMON Matrix group table entries) that describes the traffic between pairs of hosts.

# CHAPTER 4 Working with Agents, Groups, and Switches



This chapter describes how to add and modify agents, agent groups, and switches to the *ForeView RMON* ***ST*** console.

RMON agents are pre-installed on the FORE Systems' LAN switches. If the agents are not present on the hub, the hub's system software must be upgraded before using *ForeView RMON* ***ST***. Contact FORE Systems TAC for more information.

To use *ForeView RMON* ***ST*** to monitor network traffic on a segment, you should:

- Add the agent to *ForeView RMON* ***ST*** main console.
- Test the agent to ensure proper operation.
- Attach the RMON domain to the agent using Domain Manager.

Note that if you are using a network probe, you must add the agent to the probe before adding the agent to *ForeView RMON ST.* See your network probe documentation for more information.

Once you've added and tested the agent, you can then use *ForeView RMON* ***ST***'s network monitoring tools to examine segment traffic using that agent.

Network traffic can be monitored either with one or more FORE Systems' LAN Switches containing embedded RMON agents, or with one or more network probes containing RMON agents.

*ForeView RMON* ***ST*** makes it easy to add, modify, and delete agents, agent groups and switches. This chapter describes how to configure and edit agents, agent groups, and switches. For information on specific agent configuration tasks, see the following sections:

## 4.1 The Roles of Agents, Groups, and Switches

Agents on network segments continuously collect and record segment data. When you add the agent to *ForeView RMON **ST***, the *RMON **ST*** application can monitor selected portions of the segment traffic. In some cases, you can also change certain aspects of data collection in the agent, such as setting alarms.

The agents on the FORE Systems' LAN Switches are not altered when you add, delete, or modify an agent. What changes is the type of information collected and recorded by the *ForeView RMON **ST*** console.

You may want to monitor network traffic from more than one agent at a time. To do this, you define one or more agent groups. An agent group is a group of agents that *ForeView RMON **ST*** treats as a single entity. You add, edit, and delete agent groups the same way you handle individual agents.

If you want to monitor traffic at the switch level before drilling down to analyze a specific segment or group of segments, you can attach an agent to a switch. You add, edit, and delete switches the same way you handle individual agents.

If you are using a network probe, the agents must be added to the probe before you add them to *ForeView RMON **ST***.

## 4.2 Working with Individual Agents

You add, edit, and delete individual agents from the *ForeView RMON **ST*** main window, as shown in Figure 4.1. The **Agents [All]** list box, which contains the names of individual agents and selection buttons associated with those agents, is displayed on the left side of the main window. A similar list box, **Agent Groups**, is displayed in the middle of the window, between the **Agents [All]** and the **Switches** list boxes. When you first start *ForeView RMON **ST***, the **Agents [All], Agent Groups** and **Switches** list boxes are empty.

**Figure 4.1 -** *ForeView RMON* ***ST*** main window

## 4.2.1 Adding a New Agent

To add a new agent to *ForeView RMON* ***ST***, use the following procedure.

1. Select All **from** the Show option choices beneath the **Agents [All]** list box. The list box now displays all installed agents.
2. From the **Agents [All]** group of buttons, select New. The New Agent window is displayed as shown in Figure 4.2 on page 4-4.

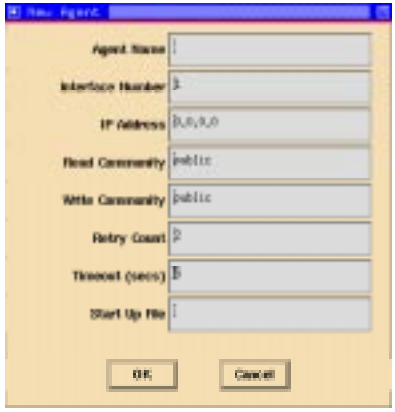



**Figure 4.2 -** New Agent window

3. Fill in the fields with the information for the agent you want to add:
   - Enter the **Agent Name** (the name you choose for the agent you want to add). The agent name can be up to 15 alphanumeric characters and is case-sensitive. You can also use dashes and underscores.
   - Enter the appropriate Interface number for the type of agent into the **Interface Number** field. Refer to the documentation for your network probe or RMON agent to determine the appropriate number. The default is 1.
   - Enter the **IP Address** for the agent. This address must be a valid IP address and must consist of numbers separated by decimal points.
   - Enter the **Read Community** string for the agent. The default read community string is **public**.
   - Enter the **Write Community** string for the agent. The default write community string is **public**.

NOTE

The read and write community strings must match the read and write community strings on the PowerHub switch, or the agent will not function. See the PowerHub software manual for information on setting SNMP communities.

- Enter the **Retry Count**. This is the number of times *ForeView RMON **ST*** tries to reach the agent if it gets no response. The value must be an integer and be equal to 1 or greater. The default value is 2 times.
- Enter the **Timeout (secs).** This is the length of time *ForeView RMON **ST*** waits before retrying an SNMP request. The value must be an integer and be equal to 1 or greater. The default value is 5 seconds.
- Enter the name of the **Startup File**. This is a script file that installs selected domains on the agent *only* when it's rebooted.

4. Click on OK to add the agent or Cancel to quit and return to the *ForeView RMON **ST*** main window.
5. Now go back to the *ForeView RMON **ST*** window. The new agent should be displayed in the **Agents [All]** list box.
6. Select the new agent.
7. Click on the Test button to confirm that the new agent is reachable. If it is, you'll see a window listing information about the agent. Testing an agent is described in the following section.



## 4.2.2 Testing an Agent's Operational Status

There may be times when you need to quickly determine if a particular agent is operational, and the date and time it became operational. This is particularly true if you have many agents operating on segments. You can easily test any agent added to *ForeView RMON **ST*** using the Test button next to the **Agents [All]** list box on the *ForeView RMON **ST*** main window. The Test function does these things:

- It performs a ping to determine whether the agent is operational.
- It tests the agent's read and write community strings.
- It reads the system interface information only when the read community string passes. Results are displayed in a dialog.

You should routinely test any new or modified agent before you use it. To test an agent, use the following procedure.

1. Select the agent you want to test from the **Agents [All]** list box on the *ForeView RMON **ST*** main window.
2. Click on Test. If the agent is operational, the agent and interface information appear in a window as shown in Figure 4.3. If the agent is not operational, the information in the dialog box tells you whether the agent can be reached, and if so, whether the read community string, the write community string, or both, has failed.


**Figure 4.3 -** Agent Test window

3. When you've finished viewing the information, click on OK.

## 4.2.3 Editing, Viewing, & Deleting Agents

There may be times when you'll want to change an agent's parameters, or review the parameters without modifying them. When you no longer need to monitor a certain part of your network, you may want to delete the agent (remove it from the *ForeView RMON **ST*** main window). In this section you'll learn how to do these three tasks.


You **cannot** rename an existing agent; this is the **only** parameter you cannot modify. To change the name of an existing agent, create a new agent with the same parameters and the name you want, then delete the original agent.

### 4.2.3.1 Editing an Agent

Once you've added an agent to *ForeView RMON **ST***, you can edit it (change its parameters) at any time. For example, you may want to change an agent's timeout or retry times to meet changing network conditions or monitoring requirements. To change one or more parameters in an existing agent definition, use the following procedure.

1. Select the agent you want to edit from the **Agents [All]** list on the *ForeView RMON **ST*** main window.

2. Select Edit. The Edit Agent window is displayed. It is the same as the New Agent window shown in Figure 4.2, except that the fields are already filled in for the existing agent.
3. Change the fields you want to edit, using the guidelines described in Adding a New Agent on page 4-3.
4. Click on OK to replace the original agent with the modified agent, or Cancel to return to the *ForeView RMON **ST*** main window without modifying the agent.
5. Select the agent you just modified. Then test the agent as described in Working with Agent Groups on page 4-8 to ensure proper operation.



### 4.2.3.2 Viewing an Agent's Parameters

You may want to review the parameters for an agent without changing them. For example, you may have forgotten the agent's timeout value. To view the values in each agent field without changing anything, use the following procedure.

1. Select the agent you want to view from the **Agents [All]** list box.
2. Click on View. The View Agent window is displayed. It is the same as the New Agent window as shown in Figure 4.2, except that the fields are filled in for the existing agent. You *cannot* edit these fields.
3. Click on OK when you're finished viewing the agent.

### 4.2.3.3 Deleting an Agent

As your network monitoring requirements change, you may no longer need to monitor a certain network segment. In this case, you might want to delete the agent from *ForeView RMON **ST***. When you delete an agent from *ForeView RMON **ST***, the actual agent remains connected to the network segment, gathering information, but *ForeView RMON **ST*** no longer monitors the data it collects. To delete an agent from *ForeView RMON **ST***, use the following procedure.

1. Select the agent you want to delete from the **Agents [All]** list box on the *ForeView RMON **ST*** main window.
2. Click on Delete.
3. When a window requesting you to confirm the deletion is displayed, click on Yes to delete the agent or Cancel to return to the *ForeView RMON **ST*** main window without deleting the agent.


When you delete an agent, it is no longer displayed in the **Agents [All]** list box. Similarly, if you deleted an agent that also belongs in an agent group, it's deleted from the group as well. To resume monitoring data from the agent, you must define it again as a new agent.

# 4.3 Working with Agent Groups

An agent group is a collection of agents that you define. You can create new agent groups, modify groups, view group definitions, and delete groups. Depending on your requirements, an agent can belong to one or more groups, or to no groups at all.

Once you've defined an agent group you can use *ForeView RMON **ST***'s monitoring and analysis tools with that group exactly the same way you would with a single agent. The difference is that you can compare traffic from different agents in the same graphical presentation. For example, if you want to monitor and compare traffic in three different segments, you can put agents on all three segments, add them to *ForeView RMON **ST***, create an agent group for them, and use Traffic Monitor to compare the traffic from all three segments on a single graph. For more information on Traffic Monitor, see Chapter 5: Monitoring the Network using Traffic Monitor.

To focus your attention on just one agent within a group, you can select Scope to select or deselect certain agents. Scope is an editing tool that lets you further narrow the scope of your tasks to just those agents you specify.

## 4.3.1 Creating an Agent Group

When you add a group of agents you simply select the agents you want to include in the group, give the group a name, and add the new group to *ForeView RMON **ST***. To create a new agent group, use the following procedure.

1. Click on New from the **Agent Groups** set of selection buttons in the main window.

A window similar to that shown in Figure 4.4 is displayed.

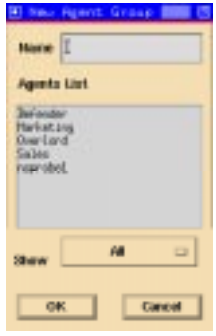



**Figure 4.4 -** New Agent Group window

2. Do one of the following:
   - If you want to see **all agents** available to be included in a group, click on the All button, displayed to the right of the Show field.
     *or*
   - If you want to see **all switch servers** available to be included in a group, click on the All button (the default), displayed to the right of the Show field, and select the Switch Servers option.
3. To select from the agents, or switch server displayed, just highlight the ones you want to include in the new agent group.
4. Enter a group name. The agent group name can be up to 15 letters, and is case-sensitive. You can use numbers, letters, dashes, or underscores in the name, but it must start with *either* a letter or a number.
5. Click on OK to add the new agent group to *ForeView RMON **ST*** and the **Agent Groups** list box on the main menu, or click Cancel to return to the *ForeView RMON **ST*** main window.



## 4.3.2 Editing an Agent Group

At any time you can add or reduce the number of agents included in a particular agent group by editing the agent group. To edit an agent group, use the following procedure.

1. Select the agent group you want to edit from the **Agent Groups** list box on the *ForeView RMON **ST*** main window.
2. Click on Edit to open the **Edit Agent** Group window.
3. Highlight the agents you want to include in the group. Deselect those that you no longer want to be in the group (they should *not* be highlighted).
4. Click on OK to edit the agent group or Cancel to return to the *ForeView RMON **ST*** main window.

## 4.3.3 Viewing an Agent Group

You may want to see which agents are included in a particular agent group. Use the following procedure to view an agent group.

#### 4.3.3.1 Viewing an Agent Group

1. Select the agent group you want to view from the **Agent Groups** list box.
2. Click on View. The View Agents Groups window is displayed. It is the same as the New Agent Group window shown in Figure 4.4, except that you can't include or exclude any agents.
3. Click on OK when you're finished viewing the agent group.

### 4.3.4 Deleting an Agent Group

When an agent group is no longer useful, you can delete the group for clarity and convenience. You can redefine the same or a similar group at a later time, if needed. Remember that an agent group is just a logical grouping. When you delete an agent group, the individual agents it included are still listed in the **Agents [All]** list box in the main window. To delete an agent group from *ForeView RMON **ST***, use the following procedure.

1. Select the agent group you want to delete from the **Agents Groups** list box.
2. Click on Delete. A window is displayed advising you to confirm that you want to delete the agent group.
3. Click on Yes to delete the agent group, or Cancel to return to the *ForeView RMON **ST*** main window without deleting the agent group.


If you delete an agent that's part of an agent group, the agent is automatically deleted from the agent group definition. For more about deleting agents, see page 4-7.

### 4.3.5 Displaying an Agent Listed within a Group

You may want to view all the agents added to *ForeView RMON **ST***, or only those agents included in a specific agent group. To view all agents added to *ForeView RMON **ST***, select the All button from the **Show** options at the bottom of the Agent list box. This is the default setting. Note that the Agent list box is titled **Agents [All]**. To view only the agents that make up a particular group, use the following procedure.

1. Select the agent group whose agents you want to view from the **Agent Groups** list box in the *ForeView RMON **ST*** main window (Figure 4.5 on page 4-11).

**Figure 4.5 -** *ForeView RMON* ***ST*** main window

2. Select the Group button from the **Show** options at the bottoem of the Agent list box. (The list box heading changes to **Agents <Group name>**.)

NOTE

If no Agent Group is selected, the **<Group name>** defaults to the first group displayed under the **Agent Groups** heading. Only agents included in the selected group are displayed in the list box.

# 4.4 Working with Switches

*ForeView RMON **ST*** uses two types of RMON support to monitor switches: mini-RMON and Roving RMON. All FORE Systems' LAN Switches have embedded mini-RMON groups that are utilized by *ForeView RMON **ST*** to monitor network switches on the hubs. In addition to mini-RMON, *ForeRunner* ES-3810 switches also support Roving RMON groups.

In many ways, a switch is similar to an agent group because *ForeView RMON **ST*** treats each port as an agent, letting you monitor each switch port as you would an agent on a network segment. For example, you can install domains on ports, set multiple alarms on specific ports, as well as scope switch port displays. You can also launch additional *ForeView RMON **ST*** tools for a more detailed analysis of traffic on a selected switch port.

In this section, you'll learn how *ForeView RMON **ST*** uses mini-RMON and Roving RMON to let you continuously monitor switched LANs and provide seven-layer RMON analysis to specific switch ports on demand.

## 4.4.1 About Mini-RMON

*ForeView RMON **ST*** uses mini-RMON to continuously monitor all ports on a switch. This mini-RMON support is embedded within the FORE Systems' LAN Switches. Mini-RMON lets *ForeView RMON **ST*** view each switch port as an RMON agent. This capability is especially important in dealing with microsegmented switched LANs. If mini-RMON was not provided, on a switch with 100 ports, you would have to set up and configure one agent for every port—one hundred agents—to continuously monitor all switch ports. But with mini-RMON support, whether embedded within the switch, or provided by an external network probe, *ForeView RMON **ST*** can monitor all switch ports simultaneously.

### 4.4.1.1 Embedded Mini-RMON

Mini-RMON strikes a good balance between visibility and overhead by embedding only the essential RMON groups—statistics, history, events, and alarms—on each switch port and skipping the groups with high resource requirements. When monitoring a switch with embedded RMON on each port, *ForeView RMON **ST*** polls the switch directly for RMON information.

Mini-RMON embedded within switches lets *ForeView RMON **ST*** continuously monitor all ports on the switch while minimizing the performance impact associated with embedding complete RMON on each port. In addition, mini-RMON provides vital statistics and alarms that can signal the *ForeView RMON **ST*** software when a more detailed analysis is needed.

#### 4.4.1.2 About Roving

Roving (or Roving RMON) refers to how *ForeView RMON **ST*** can direct full RMON analysis to any switch port you select. *ForeView RMON **ST*** implements Roving automatically, whenever you launch an application or tool that requires any of the five remaining RMON groups beyond mini-RMON: Hosts, Hosts Top N, Conversations, Filters and Data Capture. A switch supports Roving when it meets the following two requirements:

- There is an analyzer port, or a port that's not transmitting network traffic that you can designate as an analyzer port.
- The switch supports mirroring—the ability to direct a copy of traffic from a monitor port to the analyzer port where the roving probe can view that traffic.

Roving involves attaching a roving agent to the desired port on the *ForeRunner* ES-3810 or, if you have a PowerHub switch, connecting a network probe to an analyzer port on the switch, then "mirroring" traffic from a selected switch port to that analyzer port. In its most basic sense, a copy of the monitor port traffic is directed to the analyzer port where the probe or agent is attached. The probe then examines this traffic as if it were receiving the traffic directly. Although the analysis port is a static, physical connection on the switch or to the probe, *ForeView RMON **ST*** dynamically sets the monitor port to the switch port you choose to analyze.

Once *ForeView RMON **ST*** detects a problem on a port, additional data may be needed to resolve it, including extensive data captures, and network-layer host and conversation lists. You can then use Roving to bring the full RMON power of the *ForeRunner* ES-3810 to the suspect port for detailed monitoring and analysis.

For example, suppose you notice an unusually high amount of network traffic on port 12. You can run Domain Manager in Switch mode and then choose to launch Conversation List, TopN Talkers graph, or All Talkers list for port 12's RMON domain to determine the reasons for the high network traffic. At that point, *ForeView RMON **ST*** automatically roves to port 12 to analyze that traffic and retrieve the host and conversation statistics needed.

### 4.4.2 Adding a New Switch to *ForeView RMON ST*

Before you can monitor a switch, you must add it to *ForeView RMON **ST***. You add a switch to *ForeView RMON **ST*** in the same way, and for the same reason, you add an agent—so *ForeView RMON **ST*** will recognize it. This is where you define any agents you're using to monitor the switch and its associated traffic.

Then whenever you launch a *ForeView RMON **ST*** application for the switch, the display includes all switch ports, as well as any proxy, roving, and dedicated agents included in the switch definition.

### 4.4.2.1 Before You Begin

Before you begin to add a switch to *ForeView RMON **ST***, please make sure of the following:

- The switch and any agents you want to include in the switch definition are *attached* to your network and are *operational*.
- The agent you want to use as a proxy agent, roving agent, or both has been added to *ForeView RMON **ST*** and is displayed in the **Agents[All]** list box in the *ForeView RMON **ST*** main window.
- If you're using a proxy or roving agent to monitor the switch, you have connected the probe to the switch as described in the user manual of your external probe.

### 4.4.2.2 Adding the Switch

There are three Switch Type options available when you add a new switch. You can use mini-RMON or Roving RMON to monitor the switch based on your selection. The PowerHub 6000 and 7000 switches use mini-RMON and the *ForeRunner* ES-3810 uses mini- or Roving RMON. The correct switch should be selected to ensure that *ForeView RMON **ST*** will function properly. The following table shows the switch models currently supported by *ForeView RMON **ST*** and the *RMON* monitoring strategy recommended for each.

| Switch | Mini-RMON | Roving RMON |
|---|---|---|
| 3810 | X | X |
| ph_7000 | X | |
| ph_6000 | X | |


FORE Systems may have added support for more FORE Systems' LAN Switches or other switches after this manual was printed. Please contact FORE Systems TAC for additional updates.

Use the following procedure to add a supported switch to *ForeView RMON **ST***. Once you add the switch, you can monitor network traffic for any ports on the switch, as well as any dedicated agents associated with that switch.

1. From the *ForeView RMON **ST*** main window, click on the New button to the right of the list box. The New Switch window, as shown in Figure 4.6 is displayed.

**Figure 4.6 -** New Switch window

2. Fill out the top two thirds of the window according to the following information.
   - **Switch Name.** Enter a name for the switch you want to add**.** The switch name can be up to 15 alphanumeric characters and is case sensitive. You can also use dashes and underscores, but no spaces.
   - **IP Address.** Enter the IP address of the switch on the network.
   - **Switch Type.** Click on this button to pull down a menu of available switch models and select the option that corresponds to your switch type.
   - **Read Community.** Enter the read community string for the switch. The default read community is public. If the agent is on the PowerHub switch, the community strings in the **New Switch** window must match the community strings on the PowerHub switch.
   - **Write Community.** Enter the write community string for the switch. The default write community is public. If the agent is on the PowerHub switch, the community strings in the **New Switch** window must match the community strings on the PowerHub switch.

- **Retry Count.** This is the number of times *ForeView RMON **ST*** tries to reach the switch if it gets no response. The value must be an integer and be equal to or greater than one. The default value is 2 times.
- **Timeout (secs).** This is the length of time *ForeView RMON **ST*** waits before retrying an SNMP request. The value must be an integer and be equal to or greater than one. The default value is 5 seconds.
- **Roving Agent.** If you're setting up a roving or proxy agent to monitor the switch, the name of the agent *must* be displayed in this field. Select the button to the right of the field, then select the name of the agent from the **Agent List** box and click on OK. You can include this agent in the display when you're monitoring the switch. For the PowerHub 6000 and 7000 switch, this field should be blank. For the *ForeRunner* ES-3810, an agent should be added if a Roving agent has been defined.
- **Dedicated Agents.** The dedicated agent options are not currently used by the FORE Systems' LAN Switches.

### 4.4.2.3 Automatically "Learning" Switch Ports

After you add a switch, you can get *ForeView RMON **ST*** to automatically "learn" the Ethernet and Fast Ethernet ports. After *ForeView RMON **ST*** learns these ports, it creates a configuration file where this information is stored. Information in this file includes port names, numbers, interface types numbers, slot numbers, and segment speeds.

It's easy to find the configuration file containing the port definitions because *ForeView RMON **ST*** uses the switch name you specify and then adds the .swp file extension. For example, if you ask *ForeView RMON **ST*** to learn ports for a switch you've named ph7switch, the configuration file created is named ph7switch.swp. Keep in mind that for *ForeView RMON **ST*** to learn the ports on a switch, you *must first add* the switch definition (see Adding the Switch on page 4-14 for details). To easily have *ForeView RMON **ST*** learn switch ports, use the following procedure.

1. From the *ForeView RMON **ST*** main window, find the name of the switch you want *ForeView RMON **ST*** to learn port information about and highlight it.
2. Click on the Learn button to the right of the **Switches** list box.

In the status bar of the main window (bottom left corner), you'll see two messages. The first message is: `Learning ports for <switchname>....` The second message is: `Switch ports learned for <switchname>`.

Once *ForeView RMON **ST*** has learned the ports for the specified switch, you can begin using it to monitor traffic and perform other diagnostic functions, as described in this manual.

### 4.4.2.4 Editing the Switch Definition

At times, you may need to edit a switch definition. Whenever you need to do so, use the following procedure.

1. From the main window, click on the New button to the right of the **Switches** list box.
2. Edit the existing definition as necessary. For information on what type of information is required for each field, see Adding the Switch on page 4-14. Keep in mind that the Edit Switch window is identical to the New Switch window. This means that you can use the information in the referenced procedure to easily edit any switch you've defined.

NOTE

The only field you can't edit is **Switch Name.** To change a switch name, you must delete the switch definition and add it again using the desired name.

3. When you've finished making the necessary changes, click on OK to save the modified definition, or click on Cancel to close the window without saving your changes.

### 4.4.2.5 Deleting the Switch Definition

Whenever you remove a switch from the network, or if you just don't need to monitor it, you can delete it from the definitions in *ForeView RMON **ST***. To do so, use the following procedure.

1. Select the switch by clicking on the switch name in the **Switches** list box.
2. From the *ForeView RMON **ST*** main window, click on the Delete button to the right of the **Switches** list box.

The *ForeView RMON **ST*** confirmation window shown in Figure 4.7 is displayed.


**Figure 4.7 -** *ForeView RMON **ST*** confirmation window

3. Click on Yes to delete the specified switch definition or No to cancel the deletion.

# CHAPTER 5 Monitoring the Network using Traffic Monitor



Traffic Monitor is an excellent place to start monitoring or diagnosing your network. This application lets you monitor multiple sites simultaneously and monitor aggregate traffic statistics at the MAC level. Monitoring the traffic on your network with Traffic Monitor gives you a clear picture of your network's operation.

You can use Traffic Monitor to establish a baseline of "normal" or expected performance and note any deviations from that performance that might signal broader network problems. You can then launch additional *ForeView RMON* ***ST*** tools to examine these suspect areas, or simply monitor certain aspects of your network in greater detail.

Traffic Monitor gives you a top-level view of your network by monitoring selected MAC-layer statistics for the RMON agents and switches you select. By monitoring statistics such as utilization, multicasts, and network errors with Traffic Monitor, you can quickly assess your network's performance and functionality. Traffic Monitor gives you several graphical views of network traffic parameters, so you can see the flow of data through your network as it's happening. You can use Traffic Monitor to monitor network traffic patterns and see where bottlenecks are occurring; this can help you isolate and eliminate whatever is causing problems. You might use Traffic Monitor to detect high collisions, error packets, and broadcast storms, among other conditions.

For information on specific Traffic Monitor tasks, see the following sections:

# 5.1 Running Different Traffic Monitor Modes

One of Traffic Monitor's strengths is its flexibility. To ensure that you can monitor traffic on your network, regardless of its complexity, Traffic Monitor runs in different modes, depending on what you select from the main window list boxes (agent, agent group, or switch). This means that behind the scenes, Traffic Monitor intelligently launches the correct application, depending on what you choose to monitor.

The Traffic Monitor window is the same in all modes; the Traffic Monitor application does *all* the background work for you, gathering statistics without more additional user configuration. The only difference you'll see when you run different Traffic Monitor modes is the application name on the title bar of each window in the GUI. The available Traffic Monitor modes are as follows:

- **Traffic Monitor mode (basic)**. Runs in basic mode when you select a single agent or agent group shown in the *ForeView RMON **ST*** main window list boxes, then click on the Traffic Monitor icon. When you launch this mode, the title bars for each window shown in the application indicate that Traffic Monitor is operating in basic mode.
- **Switch Traffic Monitor mode**. Runs in switch mode when you select a single switch shown in the *ForeView RMON **ST*** main window **Switch** list box, then click on the Traffic Monitor icon. When you launch this mode, the title bars for each window shown in the application indicate that Traffic Monitor is operating in switch mode. When you do so, you can view all the dedicated agents defined for the selected switch (contained in the switch.lst file), plus those discovered ports (defined in the x.swp file). To save you time and effort, *ForeView RMON **ST*** automatically creates the x.swp file, if one doesn't already exist.

## 5.1.1 Features of Traffic Monitor

Traffic Monitor has many features that help you to collect statistics on the type and amount of traffic on your network. Table 5.1 lists the features and provides a short explanation of each.

**Table 5.1** Traffic Monitor Features

| Feature | Description |
|---|---|
| Display properties | Traffic Monitor displays selected network information as graphical displays. These displays give you an at-a-glance overview of your network. Under the Properties heading, you can choose to display selected network data as a 2-D bar graph, a 3-D bar graph or a three dimensional pie chart. |
| Display Transposition | This powerful feature lets you transpose both bar graph and pie chart displays to get two different views of the same data. The statistics you select are displayed as functions of different agents (default) or the agents are displayed as functions of the statistics. |
| Display Inversion | You can choose to view a bar graph in inverted form. This inverts the axes of the two bar graph displays (2-D and 3-D). Depending on the data you're displaying, you may choose to switch the x and y axes to provide a clearer picture of the data and devices you are monitoring. |
| 3-D graph Manipulation | 3-D graphs, such as a bar graph or pie chart, can be manipulated to increase or decrease the three-dimensional effect of the graph according to your preference. The elevation, depth, and angle of the displayed graph can be altered. |
| Display printout | You can print any bar graph or pie chart you're viewing in the Traffic monitor to either a printer or a file. To print the display, make sure the window containing the bar graph or pie chart you want to print is current, select **File/Print** from the menu bar, fill in the requested fields, and click **Apply**. |
| Sample rate adjustment | In the Traffic monitor, you are monitoring samples collected by network agents or switches. You can change the rate at which *ForeView RMON **ST*** polls the agents or switches by selecting the Sample menu from application's menu bar and selecting the sample rate you want. |

**Table 5.1** (Continued) Traffic Monitor Features

| Feature | Description |
|---|---|
| Additional tool access | When you want to take a closer look at a particular aspect of your network for more detailed monitoring or network diagnosis, you can launch additional tools available under the Tools menu. Tools such as Segment Zoom and Segment Statistics let you zoom in on aspects of your network and the data flowing through it for a more detailed analysis. |
| Independent displays | You can bring up several Traffic Monitor windows in order to compare statistics on different segments or agents, but each window you open uses additional *ForeView RMON* ***ST*** resources. |

## 5.2 Displaying Traffic Monitor

Use the following procedure to display Traffic Monitor from the *ForeView RMON* ***ST*** main window. Once you display the Traffic Monitor application, you can begin to monitor your network's traffic by MAC-layer statistics.

1. If you haven't already done so, log in to the network management station where *ForeView RMON* ***ST*** is installed, and run the *ForeView RMON* ***ST*** application.
2. Select an agent, agent group, or switch from those shown in the list boxes in the *ForeView RMON* ***ST*** main window and click on the Traffic Monitor icon or select Application/Traffic Monitor from the menu bar. Depending on your selection, you'll see one of two displays.


If the agent, group, or switch you want isn't listed, you may need to add it. To do so, see Chapter 4: Working with Agents, Groups, and Switches.

- If you selected an agent or agent group, you'll see one graph cluster or pie chart for each agent in the group. Figure 5.1 on Page 5-5 shows the default Vital Signs 3-D bar graph in the Traffic Monitor main window.

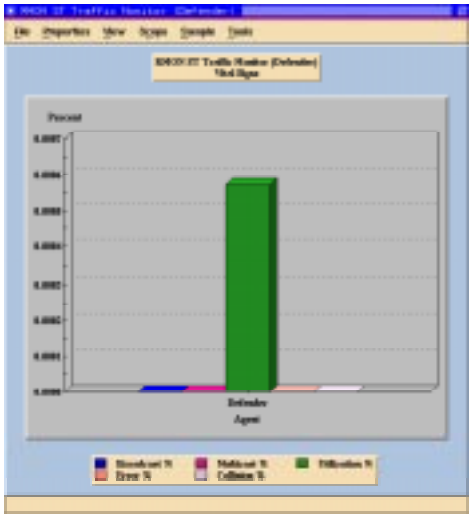


**Figure 5.1 -** Traffic Monitor main window agent display

- If you selected a switch, you'll see one graph cluster or pie chart for each port and roving agent (if any), as shown in Figure 5.2.

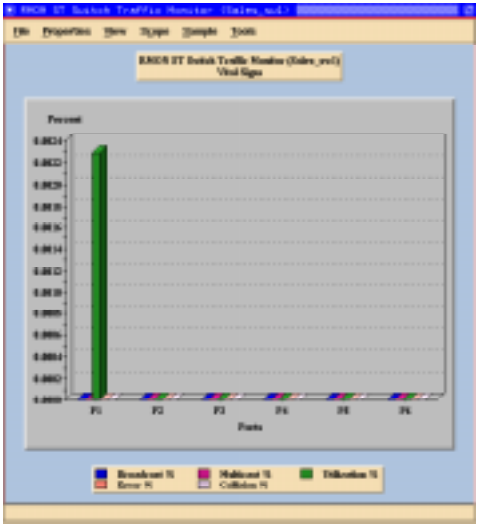


**Figure 5.2 -** Switch Traffic Monitor main window

From this main window, you now can work with Traffic Monitor in a variety of ways, described by various procedures in this chapter.

To exit Traffic Monitor at any time, just select File/Exit from the menu bar.

# 5.3 Viewing MAC-Layer Statistics

You now can select the type of data you want to monitor, the type of display, and the sample interval. Remember, although you only can monitor one data type at a time, you can simultaneously launch a number of Traffic Monitor windows, each monitoring a different statistic independent of the other windows.

## 5.3.1 Selecting the Display

To select the type of graphical display you want, select the Properties menu and then the type of display. You have three graphical display choices:

- 2-D bar chart
- 3-D bar chart
- Pie chart

### 5.3.1.1 Manipulating 3-D Graphs

Use the following procedure to manipulate the displayed 3-D graph with your mouse.

1. Move the cursor over the 3-D graph you want to manipulate.
2. Do one of the following:
   - If you have a three-button mouse, press and hold down the middle mouse button.
     *or*
   - If you have a two-button mouse, simultaneously press both mouse buttons and hold them down.
3. Drag the cursor to manipulate the graph. When the graphic is positioned the way you want it, release any mouse buttons you've pressed.

### 5.3.1.2 Resetting 3-D Graphs

Use the following procedure to reset any graph you've manipulated back to the original positions.

1. On the graph you want to reset, put the cursor anywhere in the graph.

2. To restore the original position of the graph, type the following:

+

#### 5.3.1.3 Transposing and Inverting the Display

To either transpose or invert the display, do one of the following:

- To transpose the display, select Properties/Transpose from the menu bar.
- To invert a bar graph display, select Properties/Invert from the menu bar.



## 5.3.2 Selecting the Data Type

You can now choose the type of data that you want to monitor by selecting the View menu from the menu bar and then selecting the data type. The following list gives a brief description of the data types you can monitor:

- **Utilization** - The average percentage of bandwidth utilization on the network during the sample interval.
- **Multicasts** - The number of multicasts during the sample interval, displayed as a percentage of the network traffic.
- **Broadcasts** - The number of broadcasts during the sample interval, displayed as a percentage of the network traffic.
- **Errors** - A summation of the total errors (CRC / Align, undersize, and so on) that occurred during the sample interval, displayed as a percentage.
- **Collisions** - The number of collisions during the sample interval, displayed as a percentage.
- **Vital Signs** - A summation of the general health of the network. Includes broadcast, multicasts, utilization, and error percentages. This is the default data type.
- **Size Distribution** - The percent of packets that are a given size.
- **Packet Destination** - The percent of packets being utilized for broadcasts, multicasts, and unicasts.
- **Ethernet Errors** - The percentage of Ethernet errors when monitoring an Ethernet segment.

### 5.3.3 Changing the Sample Rate

The sample rate is the interval of time *ForeView RMON **ST*** waits before polling the selected agents and updating the information displayed. You can change this sample rate to meet your needs, as shown below.

- 15 seconds
- 30 seconds
- 1 minute (default rate)
- 2 minutes
- 5 minutes

To change the sample rate, select Sample and then select one of the rates described above. *ForeView RMON **ST*** immediately uses the new sample rate to poll the segment and then update the information in the graphical display.

## 5.4 Using Scope to Look at Network Statistics

Scope lets you change the focus of your display so you can concentrate on certain statistics without having to edit your agents, agent groups, or switches. Scope can focus on specific agents in an agent group or focus on specific ports on a switch.

### 5.4.1 Using Scope to Monitor Specific Agents in an Agent Group

Scope lets you edit your display to include only specific agents when monitoring an agent group. For example, if you're monitoring an agent group consisting of five agents, you can change the scope of your display to focus on only three of those agents. To change the scope of your display, use the following procedure.

1. Select Scope from the menu bar to access the **Agents** list box in the Scope Window. The Scope window for the Agents group is displayed in Figure 5.3.


**Figure 5.3 -** Scope window (agent group)

2. Select only the agents you want to include in the display. As a shortcut, you can click on the Select All button to include all agents. Similarly, you can click on the Clear All button to deselect all specified agents.
3. Do one of the following.
   - Click on OK to see the redefined display.
     *or*
   - Select Cancel to exit Scope without applying any changes.

## 5.4.2 Using Scope to Monitor Specific Ports

If you selected a switch before launching Traffic monitor, Scope lets you edit your display to include:

- Specific ports of the switch
- The roving agent assigned to the switch (if any)
- All attached server and trunk port probes (if any)

Use the following procedure to see only specific ports, agents, or attached server or trunk port probes.

1. Select Scope from the menu bar to access the list box of all ports on the switch. The Scope window is shown in Figure 5.4.


**Figure 5.4 -** Scope window (switch information)

2. Select the ports and agents you want to include in the display. As a shortcut, you can click on the Select All button to include all ports and agents. Similarly, you can click on the Clear All button to deselect all specified ports and agents.
3. Do one of the following.
   - Click on OK to see the redefined display.
     *or*
   - Select Cancel to exit Scope without applying any changes.

## 5.5 Launching Other Tools from Traffic Monitor

You can launch other segment and domain monitoring tools directly from Traffic Monitor. To do so, first select Tools and then any of the following:

- **Segment Zoom**. Launches the Segment Zoom tool that lets you "zoom in" for a close-up view of what's happening in a domain. For details, see Chapter 7: Monitoring and Troubleshooting Single Domains.
- **Segment Statistics**. Launches the Segment Statistics Graph to provide four data views of the selected segment. For details, see Chapter 7: Monitoring and Troubleshooting Single Domains.
- **Short-Term History**. Launches the Short-Term History Graph to provide short-term historical data for the selected segment. For details, see Chapter 7: Monitoring and Troubleshooting Single Domains.
- **Long-Term History.** Launches the Long-Term History Graph to provide long-term historical data for the selected segment. For details, see Chapter 7: Monitoring and Troubleshooting Single Domains.

- **Trap Manager**. Launches the Trap Manager application that lets you monitor data thresholds by setting traps. For details, see Chapter 8: Setting Alarms Using Trap Manager.
- **Domain Manager**. Launches the Domain Manager application that lets you install or deinstall domains on an agent, as well as monitor traffic by domain. For details, see Chapter 6: Working with Domains and Domain Manager and Chapter 13: ForeView RMON ST Domains and Network Probes.
- **Agent Info**. Launches the Launch Application window that lets you select the agent for which you want information. For details, see Getting Agent Information on page 5-11.



The following options in the Tools menu are part of the RMON MIBs, but are not part of the mini-RMON subset. Therefore, they will not work with the PowerHub 6000 or 7000 systems switches without using a network probe, but are functional on the *ForeRunner* ES-3810 switch through Roving RMON.

- **Top N Talkers**. Launches the Top N Talkers Graph to provide an at-a-glance view of the top N hosts to and from the segment being monitored, in kbytes/second, for the set sample interval. For details, see Chapter 7: Monitoring and Troubleshooting Single Domains.
- **All Talkers**. Launches a tabular view of all hosts that are talking on the segment being monitored. For details, see Chapter 7: Monitoring and Troubleshooting Single Domains.
- **Data Capture**. Launches the Data Capture application that lets you capture selected data and examine single packets. For details, see Chapter 11: Decoding Captured Packets with Protocol Decode.

## 5.6 Getting Agent Information

When you want to see basic information about a selected agent, use the following procedure.

1. Select Tools/Agent Info from the menu bar to open the Launch Application window as shown in Figure 5.5.

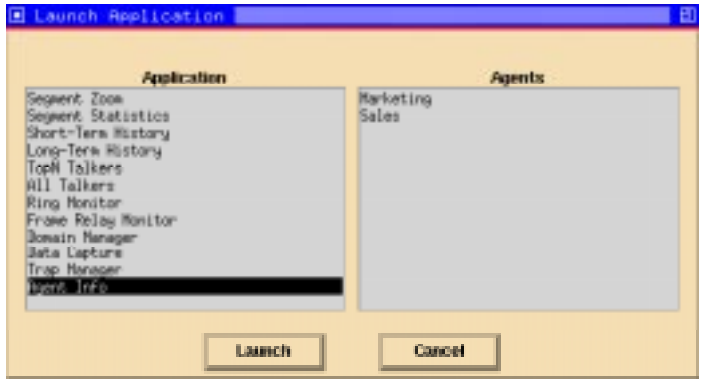



**Figure 5.5 -** Launch Application window

2. Highlight Agent Info in the **Application** list box and the agent for which you want basic information in the **Agents** list box, then click on the Launch button. The Agent information window, shown in Figure 5.6 is shown.

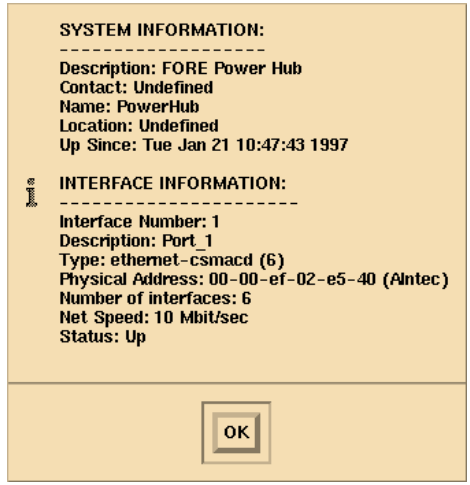



**Figure 5.6 -** Agent Information window

3. After you've finished viewing the information, click on OK to close the window.

# CHAPTER 6 Working with Domains and Domain Manager



The Domain Manager allows you to assign agents to ports on the switch using the mini-RMON and Roving RMON groups embedded in the FORE Systems' LAN switches. Once assigned, *ForeView RMON **ST*** will poll the agent for Ethernet statistics and history statistics, and let you set traps that will trigger alarms. This section explains how to add and delete domains on the FORE Systems' LAN Switches using Domain Manager, and how to display statistics and information through Domain Manager.

A domain is a subset of network activity that you can monitor using Domain Manager. *ForeView RMON **ST*** is shipped with an RMON domain which counts all traffic on the network, regardless of protocol.


A number of custom domains are defined in Domain Manager. These domains work only in conjunction with a network probe. Only the RMON agents are installed on the FORE Systems' LAN Switches.

The following sections of this chapter give more detailed information about working with domains.



You can also define your own domains if you are using a network probe in conjunction with *ForeView RMON **ST*** and the FORE Systems' LAN Switches. Domain Editor is covered in more detail in Chapter 16. Probe specific tasks are discussed in more detail in PART 2.

# 6.1 Running Different Domain Manager Modes

One of Domain Manager's strengths is its flexibility. To ensure that you can monitor traffic on your network, regardless of its complexity, Domain Manager runs in different modes, depending on what you select from the *ForeView RMON **ST*** main window list boxes (agent, agent group, or switch); Domain Manager intelligently launches the correct application depending on what you choose to monitor.

The Domain Manager window is the same in all modes; Domain Manager does all the background work for you, gathering useful statistics without more configuration required from you. Even though there are multiple applications running in the background, the only difference you'll see when you run different Domain Manager modes is the application name on the title bar of each window in the GUI. The available Domain Manager modes are as follows:

- **Domain Manager mode (basic)**. Runs in basic mode when you select a single agent or agent group shown in the *ForeView RMON **ST*** main window list boxes and then click on the Domain Manager icon. When you launch this mode, the title bars for each window shown in the application indicate that Domain Manager is operating in basic mode.
- **Switch Domain Manager mode**. Runs in switch mode when you select a single switch from the *ForeView RMON **ST*** main window **Switch** list box and then click on the Domain Manager icon. When you launch this mode, the title bars for each window shown in the application indicate that Domain Manager is operating in switch mode. When you do so, you can view all the dedicated agents defined for the selected switch (contained in the switch.lst file), plus those discovered ports (defined in the x.swp file). To save you time and effort, *ForeView RMON **ST*** automatically creates the x.swp file, if one doesn't already exist.

## 6.1.1 How Domains, Agents, & Switches Work Together

Whenever you're using agents, agent groups, or switches, you must install the domains you want before you can begin monitoring specific traffic. You can install one or many domains on an agent or switch. Likewise, you can specify a domain and install it on all the agents or switches connected to your network.

## 6.1.2 Displaying Domain Manager

Use the following procedure to display Domain Manager from the main window. Once you display the Domain Manager application, you can view, install, and deinstall domains. Use this procedure any time you need to display Domain Manager.

1. If you haven't already done so, log in to the network management station where *ForeView RMON* ***ST*** is installed, and run the *ForeView RMON* ***ST*** application (see Figure 6.1).

**Figure 6.1 -** *ForeView RMON* ***ST*** Manager main window

2. Select an agent, agent group, or switch from those shown in the list boxes. If the agent, agent group, or switch you want is not listed, you may need to add it. To do so, see Chapter 4 in this manual.
3. To launch Domain Manager and display the Domain Manager main window (Shown in Figure 6.2), either click on the Domain Manager icon, or select Application/Domain Manager from the menu bar.


**Figure 6.2 -** Domain Manager main window

4. From this main window, you can now use Domain Manager to install or deinstall a domain, view domain statistics collected, scope domains, or launch other *ForeView RMON* ***ST*** tools.

To exit the Domain Manager window and return to the main window, select File/Exit.

## 6.2 Installing and Deinstalling Domains

When you install *ForeView RMON* **ST**'s predefined RMON domain on an agent or switch, you'll see all traffic on the segment.

Before you install the RMON domain on an agent or switch, you must do the following:

- Make sure the network segment you want to monitor has an agent or switch attached and that the agent or switch is configured and connected properly and operating. See your switch or Agent documentation for configuration and connection details.
- Add the agent or switch to *ForeView RMON* ***ST*** (see Working with Individual Agents on page 4-2 or Working with Switches on page 4-12).

## 6.2.1 Installing Domains on an Agent

To install one or more domains on an agent, use the following procedure.

1. From the *ForeView RMON **ST*** main window, select the agent, agent group, or switch you want and display the Domain Manager main window (see Installing Domains on an Agent on page 6-5).
2. Click on the Install button, or select Configure/Install from the menu bar to access the Install Domain window displayed in Figure 6.3.

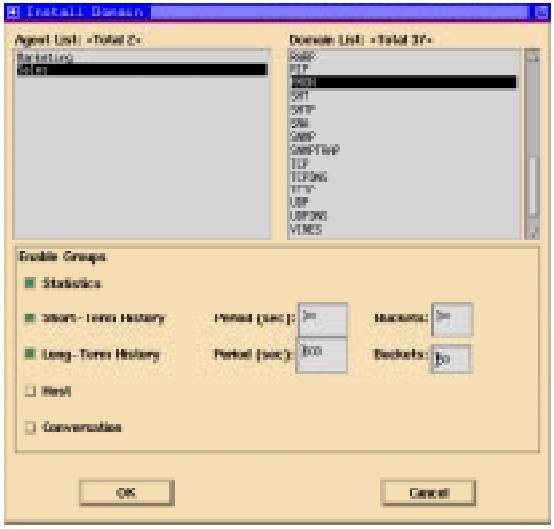



**Figure 6.3 -** Install Domain window

3. Select the RMON domain from the Domain list on the right hand column of the Install Domain window. The RMON domain is the only valid choice on FORE Systems' LAN Switches unless you are using a network probe.
4. Select the information you want to collect for the installed domains and agents or switches. You can choose to enable or disable certain statistics groups, depending on the statistics you want to monitor. You can choose to enable all statistics groups or just those you're really interested in. The following options are available:
   - **Statistics**. Collects information about packets and bytes for the entire segment. To see this information, you can choose from the Segment Stats graph for basic segment statistics, or Segment Zoom, for basic statistics *and* historical data.

- **Short-Term History**. Collects short-term historical information. To see this information, you can launch the Short Term History Graph from the Segment Zoom graph. If you specify this information, you must also specify the Periods and Buckets values. Period is the number of seconds that a bucket lasts. Bucket is the time interval when data is stored in a buffer. Defaults are 30 (Periods) and 50 (Buckets). Acceptable ranges are 1 - 3600 (Periods) and 1 - 744 (Buckets).
- **Long-Term History**. Collects long-term historical information. To see this information, you can choose the Long Term History Graph from the Segment Zoom graph. If you specify this information, you must also specify the Periods and Buckets values. Defaults are 1800 (Periods) and 50 (Buckets). Acceptable ranges are 1 - 3600 (Periods) and 1 - 744 (Buckets).
- **Host.** Collects packet and byte information for the specified host. To see this information, you can choose the Host List tool.
- **Conversation.** Collects packet and byte information about conversations between specified hosts on the segment. To see this information, you can choose the Conversation List tool.


The mini-RMON group does not include **Host** and **Conversation** statistics groups. They are available when using the Roving features of the *ForeRunner* ES-3810 switch.

5. Click on OK to install the selected domains on the specified agents or Cancel to return to the Domain Manager main window, without saving your changes.

## 6.2.2 Deinstalling a Domain

When you no longer need to monitor certain groups of statistics in a domain, or if you don't need to monitor the whole domain, you can choose to disable certain statistics groups for that domain on the agent, agent group, or switch combination, or you can disable the entire domain. Available statistics groups within any given domain, and their associated tools, are explained in Installing Domains on an Agent on page 6-5.

The procedure below explains how to deinstall a domain or statistics groups within a specific domain.

1. With the Domain Manager main window displayed, select the agent, group, or switch containing the domain you want to deinstall, and click on Deinstall or select Configure/Deinstall Domain from the menu bar.

Figure 6.4 shows the Deinstall Domain window.

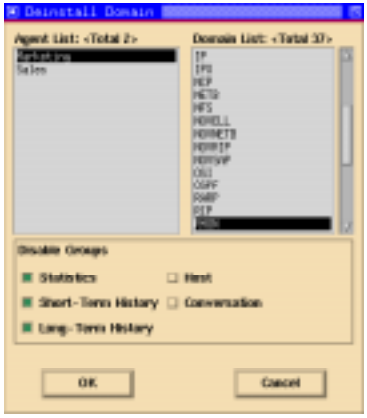



**Figure 6.4 -** Deinstall Domain window

2. Do one of the following:
   - If you want to deinstall one or more domains, go to Step 3.
     *or*
   - If you want to deinstall only a statistics group (statistics, short-term history, long-term history, host, or conversation) for a specific domain, go to Step 4.

NOTE

If you are using mini-RMON or Roving RMON on FORE Systems' LAN Switches, you have only one domain, RMON, to install or deinstall.

3. To disable one or more domains, do the following:
   - Make sure all domains you want to deinstall are highlighted in the **Domain List <Total N>** list box.
   - Select all the statistics group check boxes.
   - Go to Step 5.
4. To disable one or more statistics groups for a domain, do the following:
   - Make sure the domain containing the statistics groups you want to deinstall is highlighted in the **Domain List <Total N>** list box.
   - Select the statistics group check boxes that you want deinstalled.
   - Go to Step 5.
5. Click on OK to deinstall the selected domains or associated statistics groups or Cancel to quit without deinstalling your selections.

# 6.3 Monitoring Domain Statistics

Domain Manager monitors domains in a variety of ways. You can use Domain Manager to do the following:

- View a variety of statistics for domains and agents or switches.
- Display a sorted list of domains and agents or switches.
- Specify how often to sample the traffic and update the display.

By monitoring the traffic on your network, you can establish a baseline of "normal" or expected performance and note any deviations from that performance that might signal broader network problems. Once a domain is defined, you can use it to collect, view, and analyze network data associated with that domain. As described earlier, you must first install a domain on one or more agents, agent groups, or switches connected to the segment you want to monitor.

## 6.3.1 Understanding Statistics

When you display statistics for an agent, agent group, or switch, you'll notice that the Domain Manager list box contains these statistics shown below the headings. The following list gives you a brief explanation of what you'll find under the headings.

- **Agent/Port**. Displays the name of an agent (or names of agents within an agent group) or port number on a switch. If multiple domains are installed on an agent or switch, the list box displays each domain in a separate row.
- **Domain**. Displays the name of a domain installed on a specific agent.
- **Util%**. Displays the average percentage of network utilization on the network segment during the polling period. Displays "**----**" instead of a value if you did not enable statistics collection when you installed the associated domain.
- **PktRate**. Displays the number of packets per second on the network segment that meet the requirements of the domain specified in the same row. Displays "**----**" instead of a value if you did not enable statistics collection when you installed the associated domain.
- **STAT**. Displays ON if you enabled statistics collection when you installed the domain. Displays OFF if you did not enable statistics collection at that time.
- **STHIST**. Displays ON if you enabled statistics collection (automatically enables short-term history) when you installed the domain. Displays OFF if you did not enable statistics collection at that time.
- **LTHIST**. Displays ON if you enabled statistics collection (automatically enables long-term history) when you installed the domain. Displays OFF if you did not enable statistics collection at that time.

- **HOST**. Displays ON if you enabled host statistics collection when you installed the domain. Displays OFF if you did not enable host statistics collection at that time. These statistics are not supported by mini-RMON, but are supported on the *ForeRunner* ES-3810.
- **CONV**. Displays ON if you enabled conversation statistics collection when you installed the domain. Displays OFF if you did not enable conversation statistics collection at that time. These statistics are not supported by mini-RMON, but are supported on the *ForeRunner* ES-3810.

### 6.3.1.1 Viewing RMON Statistics



You can use Domain Manager to view RMON statistics for an agent, agent group, or switch. Once you display the statistics you want, you can also launch other tools to get further detail. The procedure below shows you how to view RMON statistics.

1. To see RMON statistics for an agent, agent group, or switch, select the one you want from the *ForeView RMON **ST*** main window, then click on the Domain Manager icon or select Applications/Domain Manager from the menu bar.

The Domain Manager main window is displayed as shown in Figure 6.5. The installed domains for the agent, agent group, or switch you selected are displayed.

**Figure 6.5 -** Domain Manager main window

2. Select the sort criterion and sample rate you want.

3. Select an option from the Tools menu to display RMON statistics for the chosen agent, agent group, or switch.

## 6.3.2 Sorting Information in the Domain Manager List Box

You can see the list box information sorted in certain ways, depending on the sort variable you specify. When you specify a variable, the list box headings don't change places, but the rows below the headings may, depending on the variable you select.

For example, if you select Domain Name as the sort criterion, the rows are displayed with domains in alphabetical order. The following list shows you the sort variables you can choose, and how the information is sorted for each.

- **Agent Name/Port**. The name of each included agent or port. Depending on what you selected, sorts numerically (ports), and alphabetically. Also, this option uses domain as a secondary sort key; this means that you'll see domains in alphabetical order per agent or port.
- **Domain Name**. The name of each included domain. When selected, sorts alphabetically. Also, this option uses Agent/Port as a secondary sort key; this means that you'll be able to look at multiple segments for a given protocol/domain. For example, if you select an agent group and sort by IP domain, you'll be able to see and compare IP traffic on all your segments.
- **Utilization**. The amount of bandwidth utilized per second. When selected, sorts from largest (top of the list) to smallest percentage. Domain Manager always defaults to this variable.
- **Packet Rate**. The number of packets per second for a specific domain. When selected, sorts from largest (top of the list) to smallest number of packets.

To change the sort order of the information in the Domain Manager list box, just select Sort and then select one of the above variables.

## 6.3.3 Sampling Information in the Domain Manager List Box

The sample rate is the interval of time *ForeView RMON **ST*** waits before polling and updating the information displayed in the list box. You can change this sample rate to meet your needs, as shown below:

- 30 seconds (default rate)
- 1 minute
- 5 minutes

To change the sample rate, select Sample and then select one of the rates described above. *ForeView RMON **ST*** immediately uses the new sample rate to poll the segment and then

update the information displayed in the Domain Manager list box.

## 6.4 Using Scope to Monitor Agents, Switches, and Domains

An agent or switch continually monitors network traffic, at the sample rate you specify, for all installed domains. When you first select Domain Manager from the *ForeView RMON **ST*** main window, the list box displays all the domains installed for the agents or switches you selected. However, you might want to monitor traffic for only certain agent / domain or switch / domain combinations.

Scope lets you edit the agent / domain or switch / domain combinations that are shown in the Domain Manager list box for the selected agents or switches. For example, you may want to be able to select the IP domain for any agent or switch quickly and easily. You can use Scope to display only the IP domain selections rather than all the configured domains. As an added benefit, Scope also helps you control the amount of SNMP-based traffic that occurs, because you're in effect polling only specific devices, instead of all devices on a segment.



### 6.4.1 Scoping Individual Agents and Domains

When you use Scope to edit the agents or switches and domains that are displayed, as long as you're in the current *ForeView RMON **ST*** session, those are the only ones you'll see. However, in any session, you can change the scope at any time. Keep in mind, though, that when you end the current session and begin a new one, you'll again see all the agents or switches and domains that are currently installed. To select the agent / domain or switch / domain combinations that are displayed in the Domain Manager list box, use the procedure below.

1. Click on the Scope button from the Domain Manager window, or select Config-

ure/Scope Domains from the menu bar.

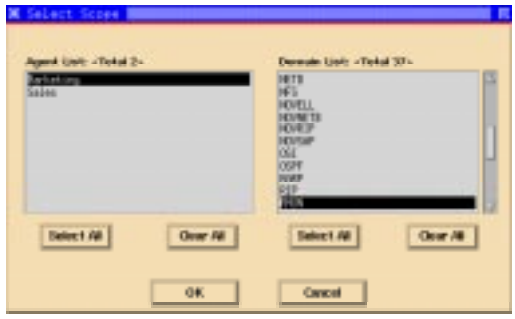



**Figure 6.6 -** Select Scope window

The Select Scope window appears as shown in Figure 6.6. All agents and domains that are currently being monitored are highlighted. The window contains two list boxes:

- **Agent List**. Displays the name of each defined agent that you're monitoring with Domain Manager. If you've selected a switch, in this list you'll see all port numbers, roving agents or attached agents, if applicable.
- **Domain List**. Displays the name of every domain currently defined in *ForeView RMON* ***ST*** and the total number of domains shown in the list box.

2. Under **Agent List**, select the agents or switches you want to be displayed in the list box on the Domain Manager window.
3. Under **Domain List**, select the domains you want to appear in the list box on the Domain Manager main window. The domains you select must be a subset of the domains that are installed for the selected agent, agent group, or switch.

NOTE

If you select a domain that isn't installed on an agent or switch, it won't be displayed in the Domain Manager list box.

4. Click on OK to see the selected agents and domains, or Cancel to leave the Domain Manager list box display unchanged.

The agents or switches and domains you selected are displayed in the list box in the Domain Manager main window. You can view the traffic information listed for each agent / domain or switch / domain combination, or use this information with other *ForeView RMON* ***ST*** tools.

### 6.4.2 Selecting or Deselecting Agents and Domains

To select or deselect a single agent from the Scope list, just click on the name. To select all agents at once, click on the Select All button under the corresponding list box in the Select Scope window. Or, to deselect all added agents, click on the Clear All button under the corresponding list box in the Select Scope window.

### 6.4.3 Displaying All Installed Domains

To quickly reset the scope to include all the installed domains for agents or switches, click on the Rediscover button on the Domain Manager main window. The scope now includes the entire set of installed domains, which are displayed in the list box.



## 6.5 Launching Other Tools from Domain Manager

You can launch other segment and domain monitoring tools directly from Domain Manager. To do so, first select Tools and then any of the following:

- **Segment Zoom**. Launches the Segment Zoom tool that lets you "zoom in" for a close-up view of what's happening in a domain. See Chapter 7 for more information on this tool.
- **Host List.** Launches the Host List tool that displays the list of hosts for the selected agent and domain. See Chapter 7 for more information on this tool. This application is not part of the mini-RMON standard and so is not supported by the embedded RMON agents on the PowerHub 7000 and 6000 switches. However, it is functional on the *ForeRunner* ES-3810.
- **Conversation List**. Launches the Conversation List tool that lets you see host conversation details. See Chapter 7 for more information on this tool. This application is not part of the mini-RMON standard and so is not supported by the embedded RMON agents on the PowerHub 7000 and 6000 switches. However, it is functional on the *ForeRunner* ES-3810.
- **Trend Reporter.** Launches the Trend Reporter application that lets you choose from predefined reports or create your own on various network events and statistics. See Chapter 9 for more information on this tool.

### 6.5.1 Printing the Domain Manager List Box

At times, you may want to the print the contents of the Domain Manager list box for your records. To print the contents of the Domain Manager list box as a report, use the following procedure.

1. Select File/Print from the menu bar to open the Print Options window, as shown in Figure 6.7.


**Figure 6.7 -** Print Options window

2. Do one of the following:
   - To print the contents of the list box to a file, select **File** as the destination, specify the directory path under **Directory**, and type the filename in the **File** field.
     *or*
   - To print the contents of the list box directly to a printer, select **Printer** as the destination, and type the printer name in the **Printer** field.
3. Click on Apply.

# CHAPTER 7 Monitoring and Troubleshooting Single Domains



Earlier chapters describe *ForeView RMON **ST*** tools that monitor multiple segments and domains. In this chapter you'll find tools that focus on a single agent and domain. You use these tools to more closely examine different aspects of network operation.

Typically, you'll first use a multi-segment, multi-domain tool to get a general idea of the portion of your network you want to monitor, then use the single-agent, single-domain tools to zero in on the portion you want to examine more closely.

The following sections of this chapter give more information on the tools available in Domain Manager to monitor and troubleshoot single domains:



## 7.1 Single Agent/Domain Tools

There are two ways to launch single agent / domain monitoring tools:

- Directly from a Traffic Monitor graph
- From the Tools menu of a multi segment / domain monitoring tool

Keep in mind that Traffic Monitor runs in three modes. Title bars shown on graphs may be different depending on the mode it's in when you run it. For more about the different Traffic Monitor modes, see Running Different Traffic Monitor Modes on page 5-2.

You can narrow your focus on specific parts of the network using the following Domain Manager tools:

- **Segment Zoom**. Displays statistical data available from a particular agent and generic domain (this tool isn't available for protocol domains). You can choose a graphical or tabular presentation.
- **Segment History**. Displays segment history as three superimposed graphs: Utilization, Collisions, and Errors. A menu option lets you switch between short-term history and long-term history from Segment Zoom.
- **Segment Statistics**. Provides the following data views for the selected segment:
  - Utilization
  - Packets
- **Short-Term History**. Provides short-term data (residing in the selected agent**)** for a period you select.
- **Long-Term History**. Provides long-term data (residing in the selected agent**)** for a period you select.

## 7.1.1 Launching Tools from Traffic Monitor Graphs

To launch single agent / domain tools, use the following procedure.

1. Do one of the following:
   - **If you're launching a tool from Traffic Monitor**, click on a bar or pie slice in the appropriate graph to select an agent.
   - **If you selected an agent through Traffic Monitor**, the Launch Application (Traffic Monitor) window is displayed as shown in Figure 7.1.

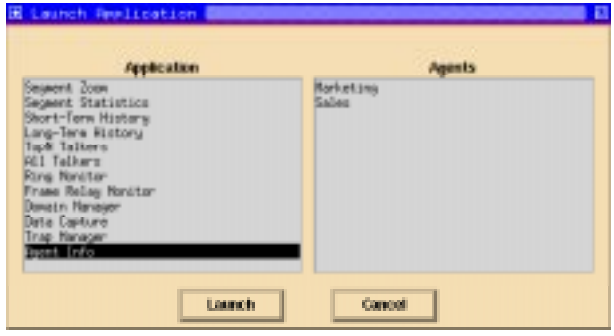



**Figure 7.1 -** Launch Application (Traffic Monitor) window

2. Highlight the following:
   - The application you want to use
   - The agent you want to select
3. Click on Launch.

If you are using an external probe, and wish to launch single agent / domain tools from Protocol Monitor, see Launching other Applications from Protocol Monitor on page D-25.

## 7.1.2 Launching Tools from the Tools Menu

In either Traffic Monitor or Domain Manager, you can launch a single agent / domain tool directly from the Tools menu. To launch a single agent / domain from the Tools menu, use the following procedure.

1. Select Tools from the application's network monitoring window menu bar and then select the segment or domain tool you want.


For all tools *except* Domain Manager, one of the Application Launch windows is displayed.

2. Select the application you want to launch, if it isn't already highlighted.
3. Select the appropriate agent and domain.
4. Click on Launch.

The selected application is displayed.

## 7.1.3 Getting Agent Information

You can view a description of the selected agent's system information and interface configuration directly from most of the graphs and lists in this chapter. To view agent information, click on the Agent Info button, if it's available, or select Tools/Agent Info from the menu bar. The Agent Information window shown in Figure 7.2 on page 7-4 is displayed.


**Figure 7.2 -** Agent Information window

## 7.2 Getting Short- and Long-Term History Graphs

Short- and long-term histories reside in the agent and show statistical histories over preset time periods. History statistics are derived from the segment statistics groups of RMON. In order to get history graphs, the agent installed must have statistics, short-term history, and long-term history groups enabled. The RMON agent is already installed on FORE Systems' LAN Switches, and you enable the collection of different RMON groups through the *ForeView RMON **ST*** application. To confirm or install these groups, see Chapter 6, Working with Domains and Domain Manager.

The default sample period for a short-term history is 30 seconds. The default is 30 minutes for a long-term history. The actual sample time is displayed at the top of the graph. You determine the number of samples, or buckets, stored in the agent when the domain is installed. See Installing Domains on an Agent on page 6-5 for more information about installing domains.

Getting either type of graph is easy; just select either Tools/Short-Term History or Tools/Long-Term History from Traffic Monitor, Segment Zoom, or Domain Manager. When you do so, the graph type you selected is displayed. For example, a short-term history graph is shown in Figure 7.3 on page 7-5.

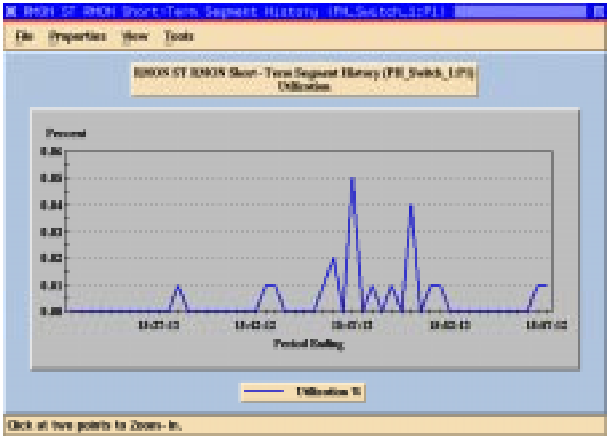


**Figure 7.3 -** Short-Term History window



## 7.2.1 Selecting Statistical Variables

You can select the statistical variable you see on either the Short-Term and Long-Term History graphs. When you do so, the x and y axes may change to fully show the variable you selected. The default variable is Utilization. To select a variable for use with either graph, use the following procedure.

1. Select the View menu. These variable selections are displayed:
   - Utilization (default)
   - Packets
   - Bytes
   - Vital Signs
   - Packet Destination
   - Errors
2. Select one of the variables. The selected graph is displayed according to the variable you chose.

## 7.2.2 Displaying History Graphs

When you collect history statistics, you can display the results in four different graph types. The default graph type is Plot. To change the graph type, use the following procedure:

1. Select the Properties menu.

2. Select the graph type. You can choose from:
   - Plot (default)
   - Area
   - 2-D bar chart
   - 3-D bar chart

### 7.2.3 Printing the History Graphs

You can print the history graphs at any time. To do so, see Printing Graph and Tabular Displays on page 7-25.

To exit the history graphs at any time, just select File/Exit from the menu bar.

## 7.3 Segment Zoom Displays

Segment Zoom displays the traffic information available from a particular agent for a single domain. Most of the displays are refreshed every update period. (The update period is user-defined.) Two displays, graphical and tabular, are available. Each display provides different information.

- The graphical view is useful in visualizing relationships and trends.
- The tabular view displays specific values for the variables you select.

You can launch Segment Zoom from Traffic Monitor or Domain Manager.

The graphical view shown in Figure 7.4 on page 7-7 is displayed by default when you launch Segment Zoom from Traffic Monitor. The tabular view shown in Figure 7.1 on page 7-10 is displayed by default when you launch Segment Zoom from Domain Manager.

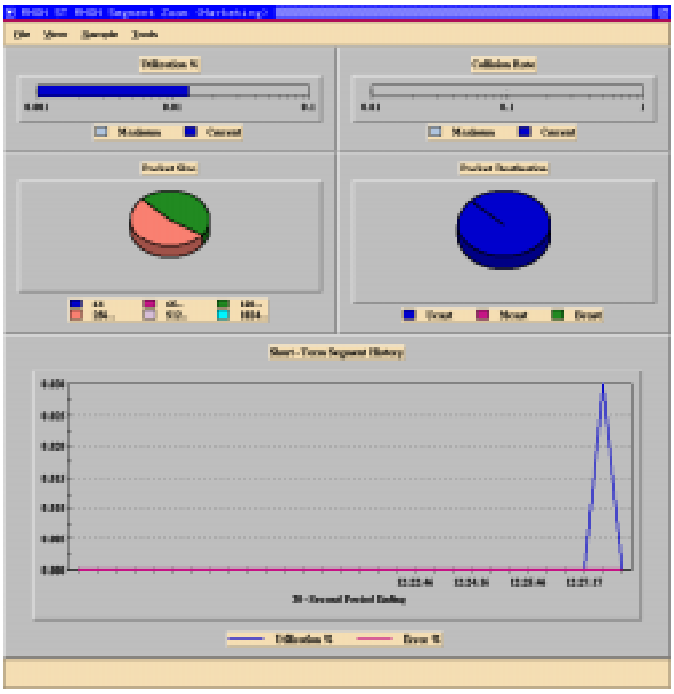


**Figure 7.4 -** Segment Zoom, graphical view

## 7.3.1 Segment Zoom Data Displays

The Segment Zoom graphical window provides the data displays described in the table below. Keep in mind that Segment Zoom displays different variables for each of the different types of agent. The displays reflect whether the network is Ethernet, WAN, FDDI, or Token Ring; differences are noted in Table 7.1.

**Table 7.1 -** Segment Zoom Variables

| This data display: | Displays: |
|---|---|
| Utilization % | both maximum and current segment utilizations as a percentage of total available bandwidth (10 Mbits/sec). For frame relay agents, two utilization % headings are displayed: DTE utilization % and DCE utilization %. Depending on the type of agent selected, these headings are customized for different types. |

**Table 7.1 -** *(Continued)* Segment Zoom Variables

| This data display: | Displays: |
|---|---|
| Collision Rate | for Ethernet only, both maximum and current segment collisions as a percentage of packets. |
| Total Packets | for FDDI only, both maximum and current token packet rate. |
| MAC Packet Rate | for Token Ring only, both maximum and current MAC packet rate. |
| Packet Size | percentages of both current and historical packet sizes as pie charts; shows six packet sizes. |
| Packet Destination | percentages of both current and historical packet sizes as pie charts. Unicast, multicast, and broadcast packets are displayed. |
| Segment History | segment history as three superimposed graphs: Utilization, Collisions, and Errors. A menu option lets you switch between short-term history and long-term history. Keep in mind that depending on the agent you select, the heading is customized. For example, if you select a frame relay agent, the heading defaults to Short-Term DTE Segment History. |

## 7.3.2 Using the Segment Zoom Graphical Display

To use the Segment Zoom graphical display, use the following procedure.

1. Launch Segment Zoom from either Traffic Monitor or Domain Manager. If you launch it from Domain Manager, switch from the text view to the graphical view using the Show Graph button on the text view window.
2. From the menu bar, select either View/Short-Term History or View/Long-Term History. The default is Short-Term History.
3. To select a data sample rate, select Sample from the menu bar and then select the rate you want. Sample rates range from 15 seconds to 5 minutes. The default is 15 seconds.
4. You can also select Tools from the menu bar, and then select from the following:
   - **Show Text**. Switches to the Segment Zoom text view.
   - **Segment Statistics**. Shows immediate segment traffic statistics in graphical form.
   - **Short-Term History**. Provides history of segment traffic statistics for a short period. The default is 30 seconds.

- **Long-Term History**. Provides history of segment traffic statistics for a longer period than Short-Term History. The default is 3600 seconds.
- **Trap Manager**. Launches *ForeView RMON **ST**'s* Trap Manager application.
- **Agent Info**. Displays information about the agent and its MIBs.

### 7.3.2.1 Identifying Problems with Segment Zoom

You can tell a lot about what's happening in a particular domain just by looking at the Segment Zoom graphical display (for example, collisions, utilization %, and other displays described earlier).

### 7.3.2.2 Printing Segment Zoom Information

To print information from the Segment Zoom window, see Printing Graph and Tabular Displays on page 7-25.

### 7.3.2.3 Exiting Segment Zoom Graphical Display

To exit the Segment Zoom graphical display at any time, select **File/Exit** from the menu bar.

### 7.3.2.4 Using Segment Zoom Text Display

The Text Display window provides additional segment traffic information in tabular form as shown in Figure 7.1 on page 7-10. Note that the selected agent and domain appear at the top of the window. The display information shown in the figure is for Ethernet; display information is different for other network and agent types.

The text display has three list boxes. The information displayed depends on the menus and selection buttons you select. To use the Segment Zoom text display, use the following procedure.

1. Select Show Text from the graphical Segment Zoom window.
   If you are in Domain Manager, the text display is displayed first.
2. Select Properties to determine the type of statistics displayed.
   You can select promiscuous statistics (default) or MAC errors.

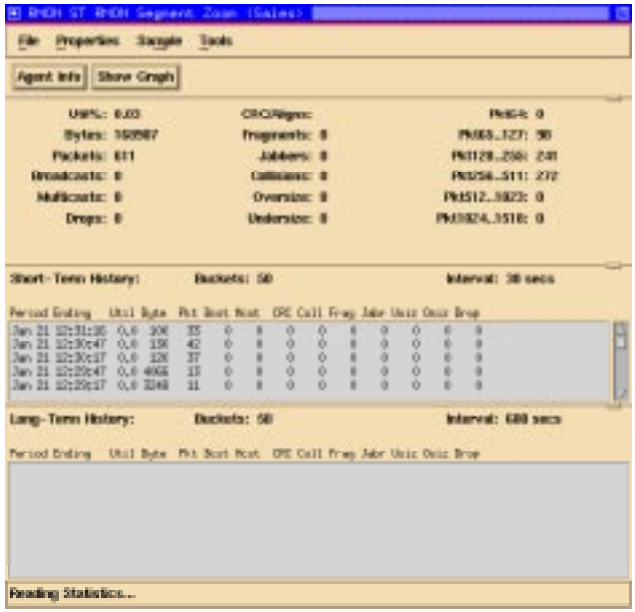



**Figure 7.1 -** Segment Zoom, tabular view

3. To select a data sample rate, select Sample from the menu bar and then select the rate you want. Sample rates range from 15 seconds to 2 minutes. The default is 1 minute.
4. You can select any of the tools available, either from those displayed when you select Tools from the menu bar, or click one of the selection buttons. Your choices are:
   - **Show Graph**. Displays the graphical representation of segment zoom.
   - **Segment Statistics**. Displays basic statistics.
   - **Short-Term History**. Available only from the Tools menu, displays a graph of segment activity for a short period of time.
   - **Long-Term History**. Available only from the Tools menu, displays a graph of segment activity for a longer period of time.
   - **Trap Manager**. Launches *ForeView RMON **ST**'s* Trap Manager application.
   - **Agent Info.** Provides information on the selected agent.

### 7.3.2.5 Segment Zoom Text Display Information

The first list box displays cumulative traffic statistics for the domain. This information is from the etherStatsTable for an Ethernet interface.

The second list box displays Buckets, Interval, and Short-Term History. This information is from the short-term history table associated with the domain.

The third list box displays Buckets, Interval, and Long-Term History. This information is from the long-term history table associated with the domain.

### 7.3.2.6 Printing Segment Zoom Text Display

If you want to print the contents of the Segment Zoom list box for your records, see Printing Graph and Tabular Displays on page 7-25.

To exit the Segment Zoom text display at any time, select File/Exit from the menu bar.



## 7.4 Host List/All Talkers

Host List gives you a complete list of the hosts and host activity that the selected agent detects for the specified domain. You can sort the list by one of the statistical values available in the Sort menu. You can use Host List to verify the number of hosts in the domain. You can also use it to determine whether a specific host is included in that domain.


Host List/All Talkers is part of the standard RMON group but is not part of the mini-RMON group. Thus it is available when using a *ForeRunner* ES-3810 switch, but is not available when using a PowerHub 6000 or 7000 switch.

Just a tabular view is available for Host List, although from Host List you can launch Tools/TopN Hosts to display the Top N Hosts graph (to provide a better idea of the Top N Host activity on the monitored segment). Also using Host List, you can select a host for the specified domain and view various statistics by selecting Tools/Host Zoom. Or, you could choose to see history information for a selected host by selecting Tools/Host History. Statistics you can display vary, depending on the tool you select, as well as the network and agent type.

Note that if the Host/group option is not enabled for the agent/domain combination you select, you'll see one of the following error messages:

```
Error accessing agent <xxx>, Domain RMON! While uploading Host Table. Error: Entry of
Group not present in Agent.
```

or

```
Host/group not enabled for this agent/domain!
```

If this happens, modify the domain installation to enable the Host/group option as described in Installing and Deinstalling Domains on page 6-4. Note that the Host Group is not supported on the PowerHub 7000 without a network probe, as it is part of the full RMON group and not part of mini-RMON.

## 7.4.1 Using Host List Tabular View

Use the Host List tabular view to see a complete list of all host activity on the segment. When you display the tabular view, you'll see cumulative counters for the information in the list box (if you choose graphical display, you'll see current values for the sample period). To see cumulative values, use the following procedure to display the Host List tabular view.

1. Select Domain Manager, Traffic Monitor, or Ring Monitor from the *ForeView RMON **ST*** main window, or launch Segment Zoom from an appropriate tool.
2. The next step depends on which tool you selected:
   - **If you selected Domain Manager**, first select an agent and domain from the list box, then select Tools/All Talkers.
   - **If you selected Traffic Monitor**, select Tools/All Talkers.
   - **If you launched Segment Zoom from another tool**, select Tools/Show Text, then Tools/Host List.

The Host List tabular view is displayed, as shown by Figure 7.2 on page 7-13.

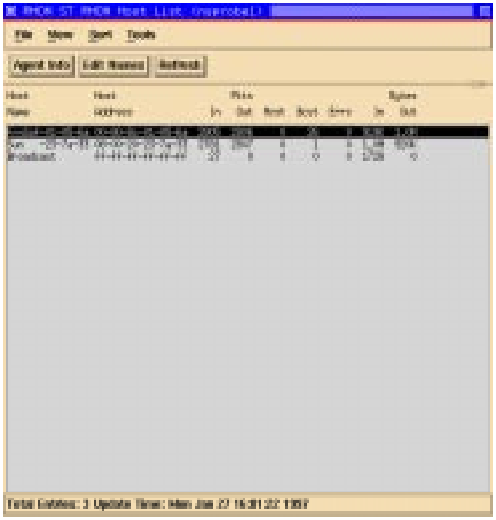


**Figure 7.2 -** Host List window, tabular view

3. From the tabular Host List view, to sort the list of hosts according to different parameters, select the Sort menu and choose from the following:
   - **Name**. Sorts by the host name. To edit a host name, highlight the name, then click on the Edit Names button. A dialog is displayed that lets you edit the name, then click on OK to save the change.
   - **Address Order.** Sorts by the address of each host.
   - **Packets In**. Sorts by cumulative number of packets inbound to the host.
   - **Packets Out**. Sorts by cumulative number of packets outbound from the host.
   - **Bytes In**. Sorts by cumulative number of bytes inbound to the host.
   - **Bytes Out**. Sorts by cumulative number of bytes outbound from the host.
   - **Multicast**. Sorts by cumulative number of multicasts inbound to or outbound from the host.
   - **Broadcasts**. Sorts by cumulative number of broadcasts inbound to or outbound from the host.
   - **Nonunicasts**. Sorts by cumulative number of nonunicasts inbound to or outbound from the host.
   - **Errors**. Sorts by cumulative number of errors in outbound transmissions from the host.

4. Depending on your needs, select any of the following (items that also correspond to a button are noted):
   - Tools/Top N Hosts
   - Tools/Host Zoom
   - Tools/Host History
   - Tools/Data Capture
   - Tools/Trap Manager
   - Tools/Agent Info (or click on the Agent Info button)
   - Tools/Edit Names (or click on the Edit Names button)
   - Tools/Refresh (or click on the Refresh button)
   - File/Print
   - File/Exit

## 7.4.2 Using Host List to View the Host History Graph

Use the Host History Graph to display statistics (utilization, packets, bytes, destinations, and errors) about a specific host for the selected agent and domain. To do so, use the following procedure.

1. Select Domain Manager or Traffic Monitor from the *ForeView RMON **ST*** main window, or launch Segment Zoom from an appropriate tool.
2. The next step depends on the initial tool you selected:
   - **If you selected Domain Manager or Traffic Monitor**, first select an agent and domain from the list box. Then select Tools/All Talkers.
   - **If you launched Segment Zoom from another tool**, select Tools/Host List.
3. When the Host List is displayed, first select the address for the host you want to see statistics for, then select Tools/Host History from the menu bar. The Host History window is displayed as shown in Figure 7.3.

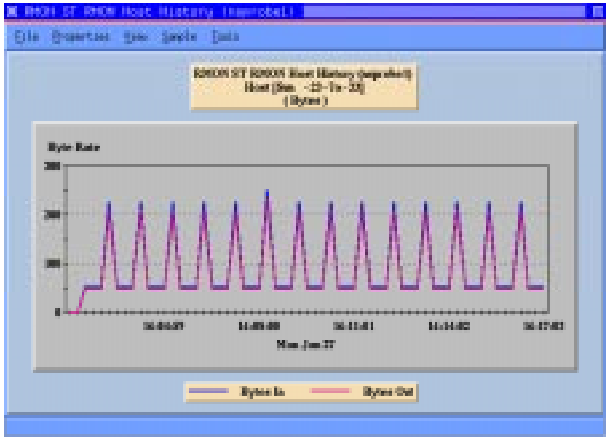


**Figure 7.3 -** Host History window

4. You can choose from five data views for the selected host. To view different statistics, select View from the menu bar and choose from the following:
   - **Utilization**. Default graph, shows all statistics (packets, bytes, destinations, and errors) for the host.
   - **Packets**. Shows the number of packets to and from the host.
   - **Bytes**. Shows the number of bytes to and from the host.
   - **Destinations**. Shows broadcasts and multicasts originating from the host only for generic domains. For protocol domains, shows nonunicasts.
   - **Errors**. Shows any errors originating from the host.

5. To set the interval between samples, click on one of the choices from the Sample menu. The range is from 15 seconds to 2 minutes. The default is 15 seconds.
6. The Tools menu lets you get agent information using Agent Info.
7. To print the contents of the Host History window, see Printing Graph and Tabular Displays on page 7-25.
8. To exit the Host Stats Graph window at any time, select File/Exit.

# 7.5 Conversation List

Conversation List is the tool you'd want to use to see more detailed information about conversations between hosts on a segment. Conversation List shows you a listing of all the hosts on a segment that are exchanging packets. For example, if host A is exchanging packets with hosts D and G, the list shows a line for the conversation between host A and host D and a separate line for the conversation between host A and host G.


Conversation statistics for the selected agent and domain must be enabled before launching Conversation List. For more about statistics groups, see Chapter 6 Working with Domains and Domain Manager.

You can also use Conversation List to display Conversation History. The Conversation History shows you the utilization, packets, bytes, and error statistics related to a specific conversational path between two selected hosts on a segment.

## 7.5.1 Viewing Host Conversations

You can view a tabular listing of host conversations: the source host, destination host, and the packet, byte, and error statistics between each host pair. To view host conversations, use the following procedure.

1. From the Domain Manager main window, select the agent or switch and domain for which you want to see host conversation information.
2. Select Tools/Conversation List.

The Conversation List window is displayed. Figure 7.4 shows the Conversation List window. Conversations between hosts for a specific domain are displayed in the window.

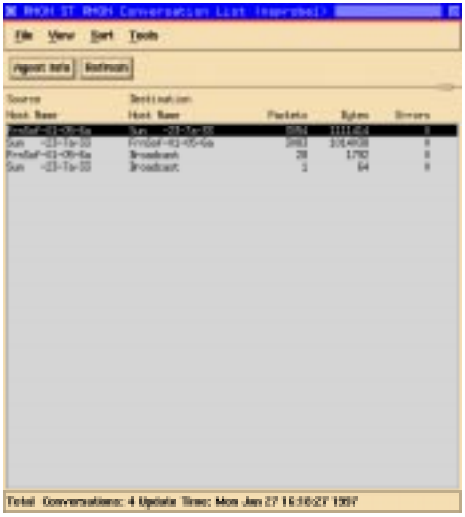



**Figure 7.4 -** Conversation List window

3. To sort the display by different display listings, select the Sort menu, then select a sort criterion. Your choices are:
   - **Source Host**. Lists conversations in order of source host to destination host.
   - **Destination Host**. Lists conversations in order of destination host to source host.
   - **Packets**. Lists conversations in order of number of packets per conversation.
   - **Bytes**. The default value, lists conversations in order of number of bytes per conversation.
   - **Errors**. Lists conversations in order of number of errors per conversation.
4. Do any of the following that applies to your situation and needs:
   - **To refresh the display**, click on the Refresh button or select Tools/Refresh.
   - **To get information about the agent**, click on the Agent Info button or select Tools/Agent Info.
   - **To view a Conversation History graph** of the same agent/domain combination, select Tools/Conversation History from the menu bar. See Section 7.5.1.1, described below.
   - **To print the contents of the window**, see Printing Graph and Tabular Displays on page 7-25.
   - **To exit the Conversation List window**, select File/Exit.

### 7.5.1.1 Using Conversation List to View Conversation History

Use the Conversation History to display statistics (utilization, packets, bytes, and errors) for conversations between selected hosts:

1. Select Domain Manager from the *ForeView RMON **ST*** main window.
2. From the agents and domains listed, select the one you want. Make sure that the agent and domain selection you chose shows a number under the CONV heading. A number under this heading indicates that conversations are enabled; if there is no number shown, you *must* click on Install and see Installing Domains on an Agent on page 6-5 for information on how to enable conversations for a domain.
3. Select Tools/Conversation List from the menu bar. The Conversation List window is shown in Figure 7.4 on page 7-17.
4. From the list displayed, select the source and destination hosts for which you want statistics displayed, and then select Tools/Conversation History from the menu bar. The Conversion History window is shown in Figure 7.5.

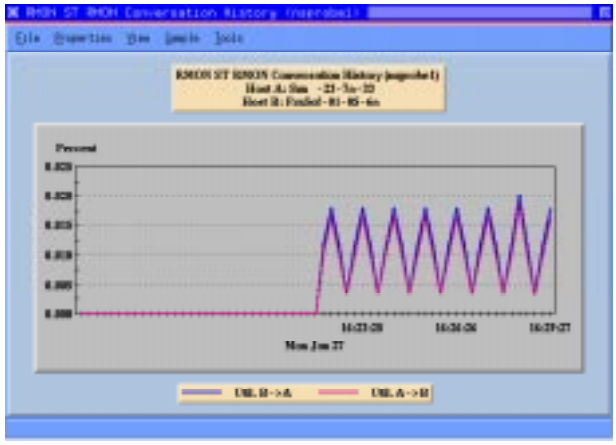


**Figure 7.5 -** Conversation History window

5. You can choose from four data views for the selected conversation. To view different statistics, select the View menu and choose from the following:
   - **Utilization**. Default, shows all statistics (packets, bytes, and errors) for the hosts.
   - **Packets**. Shows the number of packets the hosts are exchanging.
   - **Bytes**. Shows the number of bytes the hosts are exchanging.

- **Errors**. Shows any errors that occur as the hosts exchange packets. This view is available only for generic domains.

6. To set the interval between samples, click on one of the choices from the Sample menu. The range is from 15 seconds to 2 minutes. The default is 15 seconds.
7. Do any of the following that applies to your situation and needs:
   - **To get information about the agent**, click on the Agent Info button or select Tools/Agent Info.
   - **To print the contents of the Conversation History window**, see Printing Graph and Tabular Displays on page 7-25.
   - **To exit the Conversation History window**, select File/Exit.



# 7.6 Host Zoom

You can see more detailed information about a host or group of hosts for a given agent/domain by using Host Zoom. Host Zoom lists the Top N hosts with which the selected host is having conversations.

Like Host List, Host Zoom includes both graphical view *and* tabular windows. The Host Zoom graphical window displays only one of seven host traffic criteria at a time, while the tabular view displays all seven.

## 7.6.1 Using Host Zoom Tabular View

To select Host Zoom and display all seven host traffic criteria, use the following procedure.

1. From the Host List tool (see Host List/All Talkers on page 7-11), select Tools/Host Zoom. The Host Zoom default tabular view is displayed, as shown in Figure 7.6.

The agent and domain you selected are displayed at the top of the Host Zoom window. The window lists the addresses of all the hosts that the selected host is currently having conversations with, along with a number of variables. The name and address of the host you selected is displayed at the top of the window.

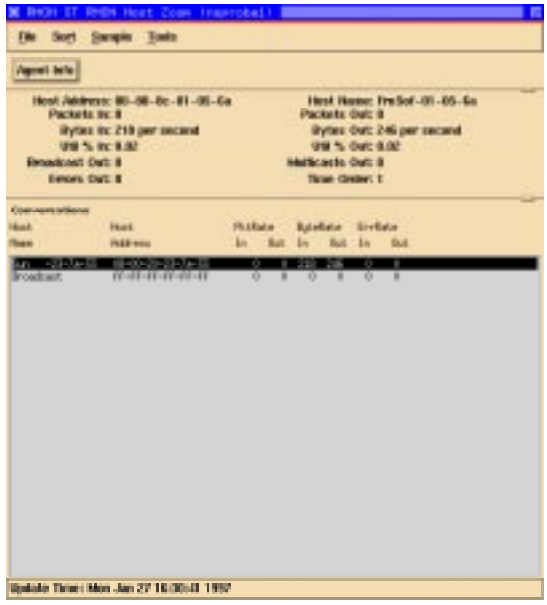


**Figure 7.6 -** Host Zoom Window, tabular view

2. To change the sort criterion, select the Sort menu. The selections are:
   - **Address**. Sorts by address of different hosts communicating to the selected host on the segment.
   - **Packets In**. Sorts by current number of packets inbound to the host.
   - **Packets Out**. Default value, sorts by current number of packets outbound from the host.
   - **Bytes In.** Sorts by current number of bytes inbound to the host.
   - **Bytes Out.** Sorts by current number of bytes outbound from the host.
   - **Errors In.** Sorts by current number of errors inbound to the host.
   - **Errors Out**. Sorts by current number of errors outbound from the host.
3. To set the interval between samples, click on one of the choices from the Sample menu. The range is from 15 seconds to 2 minutes. The default is 1 minute.
4. Do any of the following that applies to your situation and needs:
   - **To see the graphical view**, select Tools/Show Graph.
   - **To view host history**, select Tools/Host History Graph.
   - **To view conversation history**, select Tools/Conversation History.

- **To run the Data Capture application**, select Tools/Data Capture.
- **To run the Trap Manager application**, select Tools/Trap Manager.
- **To get information on the agent**, click on the **Agent Info** button or select Tools/Agent Info.

NOTE

Data Capture uses RMON groups not present in mini-RMON. Therefore, Data Capture cannot be done on the PowerHub 6000 or PowerHub 7000 without a network probe or data sniffer.



## 7.6.2 Using Host Zoom Graphical View

The Host Zoom graphical view shown in Figure 7.7 uses the same sort and sample interval criteria as the tabular view. In addition, you can switch to the tabular view from the Tools menu. The Host Zoom graphical view gives you an overview of a host's conversations, *in current values*, but it provides less detailed host information than the tabular view.

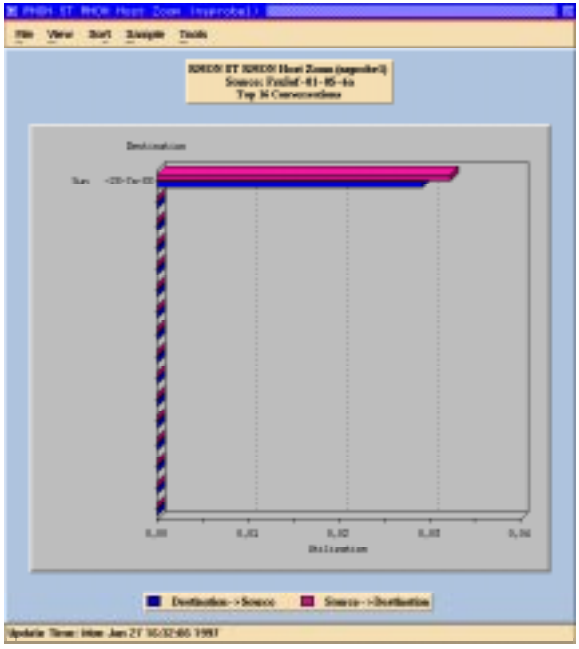


**Figure 7.7 -** Host Zoom graphical view

# 7.7 Getting Top N Talkers/Top N Hosts Graphs

Top N Talkers / Top N Hosts graphs (available in graphic view only) show the same information. However, the Top N Talkers list is a "generic" graph that includes every entity that's talking on a network segment. On the other hand, the Top N Host List shows either VLAN, DLCI, Router, or Host information (the title bar on the graph reflects your selection). The tool you select depends on the agent you select. Just remember that the information type for both graphs is the same.

Note that Top N Talkers / Top N Hosts are not a function of mini-RMON and so are supported by the *ForeRunner* ES-3810, but not the PowerHub 6000 or PowerHub 7000 unless you have a network probe attached to the network.

Getting either type of graph is easy; just select either Tools/Top N Talkers or Tools/Top N Hosts from Protocol Monitor, Traffic Monitor, Segment Zoom, Host List or Domain Manager. When you do so, the graph type you selected is displayed. For example, a short-term history graph is shown in Figure 7.8 below.

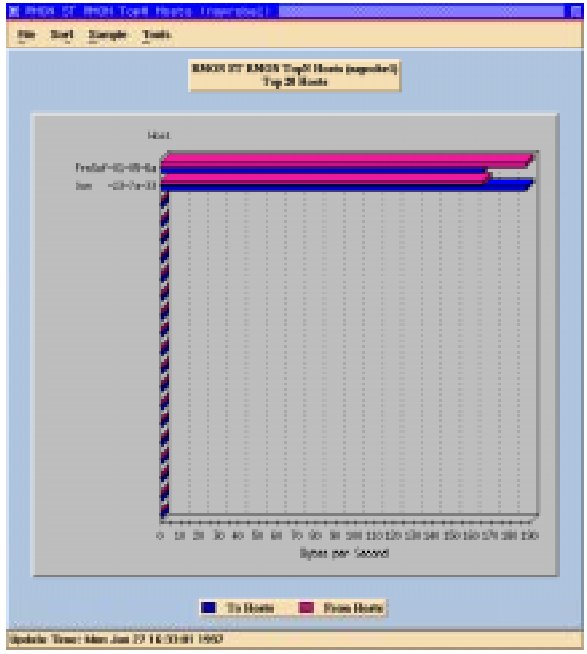


**Figure 7.8 -** Top N Hosts window

### 7.7.1 Selecting Statistical Variables

You can select the statistical variable you see on either the Top N Talkers or Top N Hosts graphs. When you do so, the x and y axes may change to fully show the variable you selected. The default variable is Bytes Out. To select a variable for use with either graph, use the following procedure.

1. Select the View menu. These variable selections are displayed:
   - Packets Out
   - Broadcasts Out
   - Multicasts Out
   - Nonunicasts Out (may be dimmed, depending on your agent selection)
   - Errors Out
   - Bytes Out (default)
   - Packets In
   - Bytes In
2. Select one of the variables.

The selected graph is displayed according to the variable you chose.

### 7.7.2 Printing the Top N Talkers/Top N Hosts Graphs

You can print the history graphs at any time. To do so, see Printing Graph and Tabular Displays on page 7-25.

To exit the history graphs at any time, just select File/Exit from the menu bar.

## 7.8 Getting a Graphical View of Segment Statistics

You can choose to see graphical views of the selected segment statistics. The available graphical segment statistics views are:

- **Utilization**. The default view, a graph by utilization percentage.
- **Packets**. A graph by number of packets per selected interval.
- **Bytes**. A graph by number of bytes per selected interval.
- **Vital Signs**. A general indication of segment health.
- **Size Distribution**. A graph by packet size.
- **Packet Destination**. A graph by packet destination.
- **Errors**. A graph by error occurrence.

When you select Segment Statistics from the Application Launch window, the Segment Statistics graph is displayed as shown in Figure 7.9. Note that the selected agent and domain appear at the top of the window.

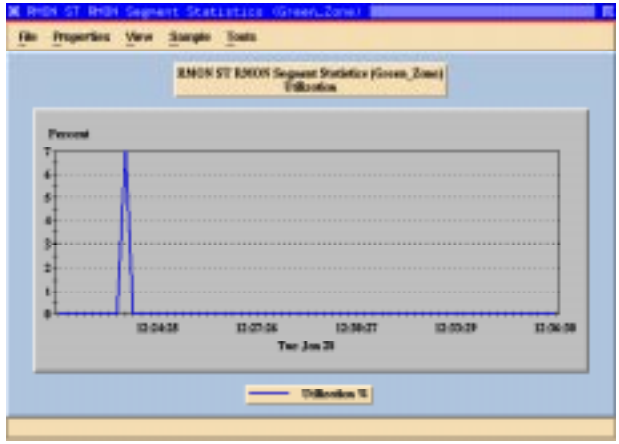


**Figure 7.9 -** Segment Statistics window

## 7.8.1 Using Segment Statistics

You can select the statistical variable you view on Segment Statistics. The default variable is Utilization. You can also define the sample interval and rate, the type of statistics displayed, and get agent information. To work with the Segment Statistics graph, use the following procedure.

1. Select the View menu and choose from one of the following variables:
   - Utilization (default)
   - Packets
   - Bytes
   - Vital Signs
   - Size Distribution
   - Packet Destination
   - Errors
2. Click on the variable you want.

3. Do any of the following that applies to your needs or situation:
   - **To run the Trap Manager application**, select Tools/Trap Manager from the menu bar.
   - **To get information about the agent**, select Tools/Agent Info from the menu bar.
   - **To display a different graph**, select Properties from the menu bar, then the graph type you want to see.
   - **To set the interval between samples**, click on one of the choices shown in the Sample menu. The range is from 15 seconds to 2 minutes. The default is 1 minute.
   - **To print the Segment Statistics window**, see Printing Graph and Tabular Displays on page 7-25.
   - **To exit the Segment Statistics window**, select File/Exit from the menu bar.



## 7.8.2 Printing Graph and Tabular Displays

The procedure for printing a graph or a tabular display is the same. Once the graph or tabular display you want to print is shown on the *ForeView RMON **ST*** console, use the following procedure to print it.

1. With the graph or tabular display you want to print displayed on the screen, select File/Print from the menu bar. Figure 7.10 shows the Print window displayed by the File/Print command.


**Figure 7.10 -** Print window

2. Do one of the following:
   - To print directly to a file, select **File** as the destination, specify the directory path under **Directory**, and type the filename in the **File** field.
     *or*
   - To print directly to a printer, select **Printer** as the destination and type the printer name in the **Printer** field.
3. Click on Apply.

# CHAPTER 8 Setting Alarms Using Trap Manager



An *alarm* is a predefined condition based on either rising or falling data thresholds, or both. When this condition occurs, it's called a *trap*. With Trap Manager, you can set multiple alarms on selected events associated with any RMON-MIB variable. You can set the same alarm on multiple agents and switches, or multiple alarms on the same variable. When you set an alarm on a network device, the alarm detects a trap when it occurs, and sends a trap message to *ForeView RMON* ***ST*** or any valid IP address specified. You can perform such monitoring when you suspect a fault in the segment or device, or just to be notified if it develops problems.

When you configure the agent or switch to send the trap message to the *ForeView RMON* ***ST*** console, the Alert Monitor icon on the *ForeView RMON* ***ST*** window blinks until you acknowledge it by selecting it. You can also create UNIX script files to take a particular action once a trap occurs.

In Trap Manager you can easily add, modify, and view alarms, as well as remove alarms you no longer need. You can also save alarm configurations in text files under names that you define. You can then retrieve these configuration files to reset or modify the alarm at any time, or set the same trap on other agents or switches.

The following sections provide more information on the Trap Manager application.

# 8.1 Understanding Alarm Basics

An alarm is a definition of a condition you set on a variable. These variables are actually counters, and the condition you monitor them for is a rising or falling data value, or both. You define this condition in Trap Manager by adding an alarm. The alarm configuration not only includes the rising and falling thresholds you set, but other specifications, such as the type of trap message to send, what to include in the trap message, the action to take once the event, or trap, has occurred and where to send the trap message (who should be notified).

## 8.1.1 Setting Rising and Falling Thresholds

When you configure an alarm, you must specify when you want the trap message generated. You can choose any of the following:

- **Rising Threshold**. When the current sampled value is greater than or equal to this threshold, and the value of the last sampling interval was less than this threshold, the agent generates a single trap message. It does not generate another such trap message until the sampled value falls below the Falling Threshold, then rises above the Rising Threshold.
- **Falling Threshold**. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, the agent generates a single trap message. It does not generate another such trap message until the sampled value rises above the Rising Threshold, then falls below the Falling Threshold.
- **Either**. The agent generates a trap message when either the rising or the falling threshold is reached.

## 8.1.2 Defining Trap Messages

When you're adding or modifying an alarm in Trap Manager, you can define trap messages for each threshold type—rising and falling—to include specific information that the agent sends as part of the message when the trap occurs. This information includes:

- **Trap Description.** This is a text string of up to 127 characters that is sent as part of the trap message to the reporting console, or the IP address you specify. When the *ForeView RMON **ST*** console receives a trap message, the Alert Monitor blinks until you select it, then displays this text message. The default descriptions are "Falling Threshold Reached" and "Rising Threshold Reached."
- **Value.** This is the value that triggers the trap.

- **Severity.** This is a relative rating of the severity of the trap. The value range is a decimal number from 0-99. The severity rating of a trap appears as part of the trap information displayed in the Alert Monitor. You can also pass the severity rating as an argument to script files you execute when a trap occurs. See Using Traps to Execute UNIX Script files on page 8-13 for more information about executing UNIX script files.
- **Program Information.** You can also use UNIX script files to take a specific action when a trap occurs. You simply define the name and path of the file when adding the alarm and the agent will send this information as part of the trap message. See Using Traps to Execute UNIX Script files on page 8-13 for further details.



## 8.2 Starting Trap Manager

Use the following procedure to start Trap Manager from the *ForeView RMON **ST*** main window. Once you display the Trap Manager application, you can set alarms on the agents or switches you selected to monitor selected variables for specific conditions.

1. Log in to the network management station where *ForeView RMON **ST*** is installed, and run the *ForeView RMON **ST*** application.
2. Select the agent, agent group, or switch on which you want to set the alarm.
3. Click on the Trap Monitor icon or select Application/Trap Monitor from the menu bar.


The Trap Manager list box contains several headings with corresponding values. Refer to Adding Alarms on page 8-6 for an explanation of each of these values.

The Trap Manager main window, as shown in Figure 8.1 on page 8-4 lists all alarms set on the selected agent. Note that the name of the selected agent is displayed in the title bar.

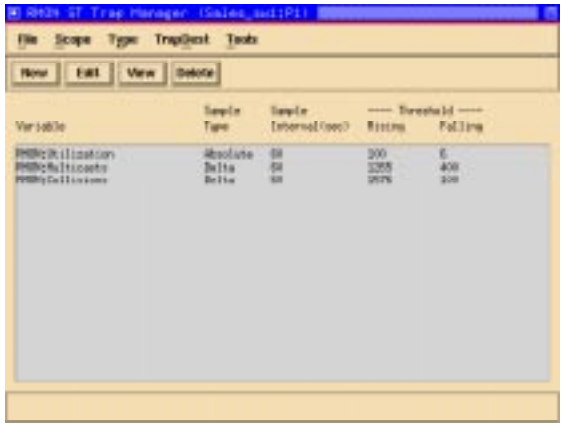



**Figure 8.1 -** Trap Manager main window

4. From this main window, you now can add, modify, view, or delete alarms to monitor and alert you of specific conditions when they occur.

## 8.2.1 Selecting the Type of Network Variable to Monitor

Before adding an alarm, you have to specify the type of variable you want to monitor. You do this from the Trap Manager main window by selecting Type from the menu, then selecting either Domains or Resource Monitor. However, because the RMON standard does not support Resource Monitor, you must select Domains unless you are using a NETscout Probe.

When you choose to monitor Domains, the list box in Trap Manager's main window displays all alarms set on domain-related statistics for the selected agent. When you add the alarm, you can choose from a variety of network statistics relevant to the type of network you're monitoring. For details on the variables you can set alarms on when selecting Domain, see Selecting Statistic Variables on page 8-11.

## 8.2.2 Changing the Scope of Your Display

If you selected an agent group before launching Trap Manager, the Trap Manager main window displays the alarms set on the first agent in the group by default. The name of the agent for which you are viewing trap information is displayed in the window's title bar. You can choose to view trap information for another agent in the group by using the following procedure.

1. From the Trap Manager main window, select Scope/Agent. The Scope Agent window is displayed.

2. Select the agent for which you want to view trap information.
3. Click on OK.

### 8.2.2.1 Printing the Display

You can print the contents of the list box in the Trap Manager's main window to either a printer or a file. To print the display, use the following procedure.

1. Select File/Print from the menu bar to access the Print Options box. Figure 8.2 shows the Print Options box.


**Figure 8.2 -** Print Options box

2. Do one of the following:
   - To print the data to a file, select File as the destination, specify the directory path under **Directory**, and type the filename in the **File** field.
     *or*
   - To print the data directly to a printer, select Printer as the destination, and type the printer name in the **Printer** field.
3. Select Apply.

## 8.3 Using Trap Manager to Set Alarms

In this section, you'll learn how to monitor your network for specific conditions by setting alarms on selected statistics using Trap Manager.

## 8.3.1 Adding Alarms

Once you've launched Trap Manager from the *ForeView RMON **ST*** main window, you can set alarms on the agent, agent group, or switch you selected. When you want to add an alarm to an agent, use the following procedure.

1. Select the agent or switch on which you want to set the alarm, and launch Trap Manager as described in the previous section. Figure 8.1 on page 8-4 shows the Trap Manager main window.
2. Select Type/Domain from the menu bar.


Because mini-RMON does not support the Resource Monitor, the Resource Monitor option is grayed out unless a NETscout Probe is configured and attached to the network.

3. Click on the New button or select Tools/New from the menu bar. The New Alarm window is displayed as shown in Figure 8.3.

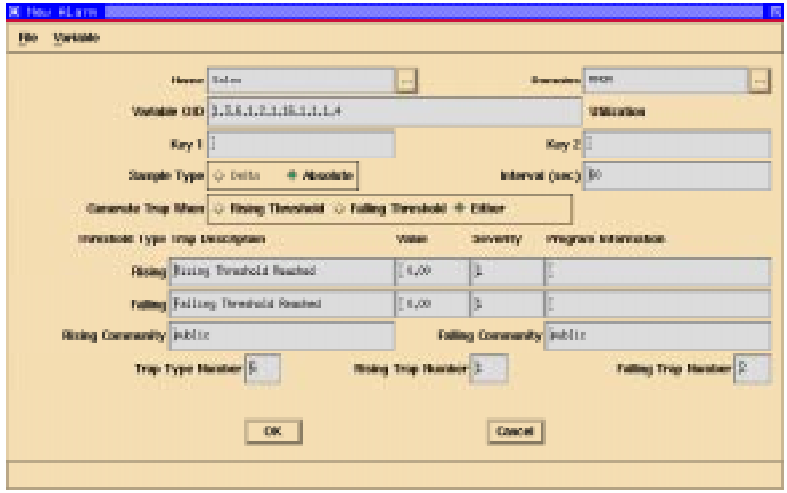



**Figure 8.3 -** New Alarm window

4. In the Name field, the name of a single agent or switch is automatically displayed, unless you chose an agent group before launching the application. If you selected an agent group, do the following:

- Select the button to the right of the field to display the Select Agent window that shows a list box containing all agents in the group.
- Select the agents you want to set the alarm on, then click on OK. If you selected a single agent, the name of the agent is displayed. If you chose more than one agent, `<<multiple selected>>` is displayed in this field instead of an agent name.

5. Just to the right of the **Name** field is a field named **Domains**. To fill in the field, do the following:
   - Click on the button to the right of the Domains field to display the Select Domain window, shown in Figure 8.4.

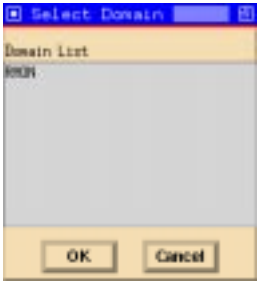



**Figure 8.4 -** Select Domain window

   - In the Select Domain window, highlight the domain you want and click on OK. The domain name you selected is now displayed in the **Domains** field.

6. From the menu bar, select Variable to access the New Alarm Window.

Trap Manager displays a list of variable statistics you can choose from. For each statistic group you select, you'll see a submenu of specific variables you can select. For more about these submenus and the variables you can monitor for a specific condition, see Selecting Statistic Variables on page 8-11.

7. Use the following table to fill in the remaining fields in the New Alarm window, then go to Step 8.

| This selection field: | Lets you specify, or displays: |
|---|---|
| Variable OID | the unique object identifier of the variable on which you want to set the alarm. To specify this variable, select Variable/<statistic group> from the menu bar. Each statistic group has a submenu of available counter variables, as shown in Selecting Statistic Variables on page 11-11. This field is filled in automatically after you select the variable on which you want to set a condition. The variable name is displayed to the right of this field. |
| Key 1<br>(Applies to Roving RMON only) | the host address when monitoring host statistics, or the source address in the case of conversation statistics. Both are available when selecting Domain as the data type. |
| Key 2<br>(Applies to Roving RMON only) | the destination address when monitoring conversation statistics, available when selecting Domain as the type. |
| Sample Type | Delta or Absolute. Determines whether the alarm is triggered on a change in data rate (Delta), such as a change in packets per second, or an absolute value (Absolute), such as the number of packets counted. |
| Interval (sec) | the interval, in seconds, that must pass before the agent samples the data and compares it with applicable rising and falling thresholds. The value must be a decimal number. The allowed range is 1 - 3600 seconds. |
| Generate Trap When | **Rising Threshold**, **Falling Threshold**, or **Either**. Values must be in decimal form and must be within the range of the variable being monitored. The default threshold is **Rising Threshold**. |
| Threshold Type Trap Description | either or both **Rising** and **Falling** fields. Type the text string you want to be sent as part of the trap message when the threshold is exceeded. You can enter up to 127 characters.<br>You must also complete the Value, Severity, and Program Information fields, described below, for each field type you select here. |

| This selection field: | Lets you specify, or displays: |
|---|---|
| Value | the value that triggers the trap. Values must be a decimal number. The ranges allowed depend on the variable selected. |
| Severity | the relative rating of the trap's severity. The value range is from 0 - 99, decimal. The severity rating of a trap appears as part of the trap message sent by the agent. |
| Program Information | the name of the UNIX script file you want to execute when a trap is detected. Using the Program Information option, you can use a trap to trigger actions in *ForeView RMON **ST*** or UNIX. |
| Rising Community | that trap messages are sent to each host registered for the community specified when a rising threshold is reached. The host where you added the alarm is automatically registered. |
| Falling Community | that trap messages are sent to each host registered for the community specified when a falling threshold is reached. The host where you added the alarm is automatically registered. |
| Trap Type Number | the type of trap message sent. This is a standard SNMP 0-6 trap-type number. |
| Rising Trap Number | a number you define to identify the trap as rising type. |
| Falling Trap Number | a number you define to identify the trap as falling type. |

8. Click on the **OK** button to save the configuration and add the new alarm.

### 8.3.1.1 Saving Alarm Configurations

You can save alarm configurations in text files under names that you specify. This capability lets you retrieve the same configuration for use at a later time. For instance, you may want to add the same alarm on several agents that are not part of the same group, or on several switches; or modify some aspect of the existing configuration. Use the following procedure to save the alarm configuration to a file.

1. From the New Alarm window, select File/Save As from the menu bar. This opens the Enter File Name window shown in Figure 8.5 on page 8-10.

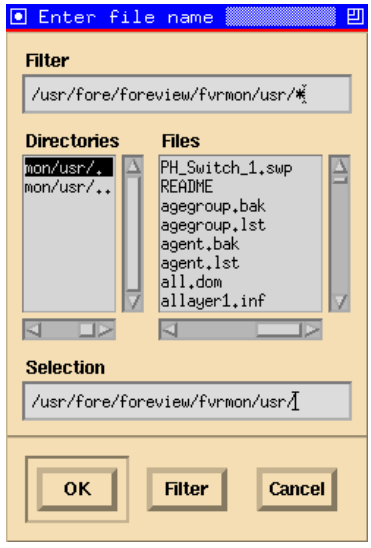



**Figure 8.5 -** Enter file name window

2. Enter the name and path of the file in the **Selection** field, or browse for a specific path or file by using the scroll bars associated with the **Directories** and **Files** list boxes. You can also focus your search to a specific file name or type by entering a wildcard search in the Filter field and clicking on Filter. For example, if you enter *.cfg in the Filter field and click on OK, you'll see only files with a .cfg extension.
3. Select OK to save the file under the specified name.

### 8.3.1.2 Retrieving Alarm Configurations

To retrieve an existing alarm configuration, use the following procedure.

1. From the New Alarm window, select File/Open from the menu bar to access the Enter File Name window shown in Figure 8.5.
2. Enter the name and path of the file you want to open in the Selection field, or browse for a specific path or file by using the scroll bars associated with the **Directories** and **Files** list boxes. You can also focus your search to a specific file name or type by entering a wildcard search in the **Filter** field and clicking on Filter.
3. Select OK to open the name of the file you've specified in the selection field. The alarm configuration information is imported into the appropriate fields.

## 8.3.2 Selecting Statistic Variables

Trap Manager lets you choose a variety of variables from a number of statistic groups. You select a statistic group from the Variable menu when adding or modifying an alarm. Choices that don't apply to the type of network segment are grayed out. Mini-RMON on the FORE Systems' LAN Switches currently support only the Ethernet Statistics group. This group should be selected from the variable menu choices when working with *ForeView RMON **ST*** and FORE Systems' LAN Switches.

The following figure shows the submenu for the Ethernet Statistics group. If you choose this group of statistics, you'll have the variables shown in Figure 8.6 that you can use to set alarms.



NOTE

Remember, if certain choices are grayed out (dimmed), they don't apply to the network segment or data type you choose.


**Figure 8.6 -** Ethernet statistic variables

### 8.3.2.1 Viewing Alarms

You can view the complete alarm configuration of any trap you've set on an agent in Trap manager. To view a particular trap displayed in the Trap Manager main window, select the trap you want to view from the list box and select the View button, or select Tools/View from the menu bar.

## 8.3.3 Modifying Alarm Configurations

Trap Manager lets you modify any of the parameters of an existing alarm configuration. You may want to change the rising or falling threshold value, destination address, or even specify a new script file to execute when the trap occurs. To modify an existing trap, use the following procedure.

1. Select the trap you want to edit from the list box in the Trap Manager main window, and click on the Edit button or select Tools/Edit from the menu bar. The Edit Alarm window is displayed with the complete alarm configuration of the selected trap as shown in Figure 8.7.

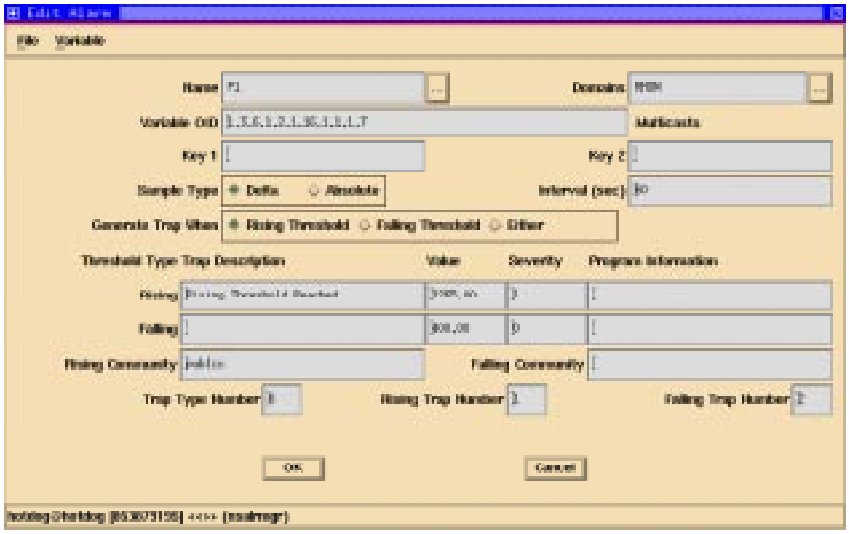



**Figure 8.7 -** Edit Alarm window

2. Make changes as necessary (see page 8-8 for descriptions of the fields on this screen and their associated values).
3. Once you've finished modifying the alarm, select OK to accept the changes or Cancel to leave the configuration unchanged.

## 8.3.4 Deleting an Existing Trap

You can remove any existing traps you no longer need by selecting the trap you want to remove from the list box in the Trap Manager main window, and selecting the Delete button, or Tools/Delete from the menu bar. A dialog box is then displayed prompting you to confirm the deletion. Select OK to delete the trap, or No to cancel the deletion.

## 8.4 Using Traps to Execute UNIX Script files

When an alarm condition occurs, the alarm generates a trap. The agent sends the trap to the IP addresses you specified when adding the alarm. If it's a *ForeView RMON **ST*** console, it causes the Alert Monitor icon on the *ForeView RMON **ST*** Main window to blink repeatedly until you click on it to display the Alert Monitor window.

You can also use traps to execute UNIX script files. These script files can perform alarm functions, such as sending mail messages or printing the trap information. They can also perform actions in the network, such as changing the speed of a router. You can pass two variables from the trap to your UNIX script file: the agent name, and the severity of the trap.



For example, you may want to automatically change the speed of a WAN router if utilization reaches a certain threshold. You can write a script to change the router speed if an alarm based on utilization triggers a trap. As a second example, you can generate a snapshot of the network segment if a certain threshold is reached. You can do this by writing a script file that runs the command line utility **dvsnap** when a certain threshold is reached.

Finally, you might want UNIX to sound an audible alarm and flash an onscreen message if a severity 1 trap occurs. The following sample script file sends a mail message when a trap is received.

```
#
# Sample shell script to be executed upon trap reception
#
# This sends a mail message to the user showing the top hosts
& conversations
#
echo High utilization trap received from agent $1, priority $2
> temp.$$
echo Top 10 hosts: >> temp.$$
$NSHOME/bin/dvsnap $1 ALL HOST 30 10 >> temp.$$
echo Top 10 conversations: >> temp.$$
$NSHOME/bin/dvsnap $1 ALL CONV 30 10 >> temp.$$
mail 'whoami' < temp.$$
rm temp.$$
```

To use traps to execute Unix script files, use the following procedure:

1. Write the UNIX script file.
   Remember that you can use both the agent name and the severity level from the trap you want to use to execute the script file.
2. Create the alarm in Trap Manager as described in this chapter (see *Using Trap Manager to Set Alarms* on page 8-5).

3. Enter the name of the script file in the appropriate Program Information field. You can have *two* separate files, one for a rising threshold and one for a falling threshold.
4. Add the alarm. The script file executes each time the alarm creates a trap.

To exit Trap Manager at any time, select File/Exit from the menu bar in the Trap Manager main window.

## 8.5 Viewing a List of Traps Using Alert Monitor

The trap list displays all the messages sent on the date shown in the date field at the top of the Alert Monitor window. Each local agent also logs traps, and you can gain access to them through an inquiry to the specific agent.

When an alarm occurs, the Alert Monitor alarm clock icon at the bottom of the *ForeView RMON **ST*** main window flashes until you acknowledge it by clicking on the icon. Click on the icon a second time to display the Alert Monitor window. To view a list of traps, use the following procedure.

1. Select Alert Monitor from the *ForeView RMON **ST*** main window. The Alert Monitor window is displayed in Figure 8.8.


**Figure 8.8 -** Alert Monitor window

2. Using the buttons to the right of the date field at the top of the Alert Monitor window, select the date for which you want to view traps. A list of traps recorded for that day is displayed in the list box.
3. If you want to view information for a specific trap, select the trap in the list box. Information on that trap is displayed in the box beneath the list box.

## 8.5.1 Deleting a Trap in Alert Monitor

To delete a trap in Alert Monitor, select the trap you want to remove then click on the Delete button, or select Tools/Delete from the menu bar. A dialogue box is then displayed prompting you to confirm the deletion. Select OK to delete the trap, or No to cancel the deletion.

## 8.5.2 Refreshing the Alert Monitor Display

You can update the information in the list box to show new traps. To do so, click on the Refresh button.

## 8.5.3 Printing Trap Information from Alert Monitor

You can print the contents of the Alert Monitor list box for future reference. To print the contents of the Alert Monitor list box, follow the printing procedure outlined in Printing the Display on page 8-5.

## 8.5.4 Exiting Alert Monitor

To exit the Alert Monitor, select File/Exit from the menu bar.

# CHAPTER 9 Logging and Reporting with Trend Reporter



*ForeView RMON **ST***'s Trend Reporter enables you to log and report various statistics related to your network. Trend Reporter is based on a relational database, which means that you can make ad hoc queries to information contained in any of the database's tables, set up automatic report generation, choose reports based on detail or summary data, and define how long detail or summary information stays in the database. Trend Reporter includes a bundled Structured Language Query (SQL) server.

Trend Reporter lets you structure reports to specific needs. The information in this chapter explains how Trend Reporter works. Chapter 10 explains more about working with and submitting ad hoc queries.

The following sections provide more detailed information on the Trend Reporter application:



## 9.1 How Trend Reporter Works

Trend Reporter is built upon a relational database, instead of flat files. Within the database are numerous tables containing different information. To access information in the database tables, you use SQL queries, whether interactively (typed on a command line) or submitted through Trend Reporter's GUI.

If you opt to use Trend Reporter's ad hoc query capability, you'll need to be familiar with SQL. SQL's queries are easy to use and understand; an example SQL query to an employee database table might look something like this:

SELECT LastName, FirstName, Extension FROM employee_table WHERE FirstName = 'David' ORDER by LastName


If you're not familiar with SQL, it's an ANSI/ISO standard that lets you use English language queries to extract or show information contained in the database. If you want to submit ad hoc queries for customized reports, you need a basic knowledge of how to structure SQL queries. For more about using ad hoc queries and for sample queries, see Chapter 10: Customizing Trend Reporter.

## 9.1.1 Using Trend Reporter's SQL Server

Trend Reporter includes a bundled SQL server, licensed from Hughes Technologies. The SQL server must run locally on the host that's also running *ForeView RMON **ST***.

The database that's located in the SQL server is a collection of tables that you access using SQL queries. Report tables are available to you and display information that you request through the GUI queries.

## 9.1.2 More About Trend Reporter's Database Tables

Trend Reporter's tables contain statistics for all agent/domain pairs. This feature allows SQL queries you submit to span multiple agents and domains if required.


For more about the structure of Trend Reporter's tables, see Understanding Trend Reporter's Table Schemata on page 10-9.

Trend Reporter uses the following types of report tables.

- Ethernet segment statistics
- Host statistics
- Conversation statistics

Each report table type can be classified into one or more of the following categories:

- **Segment**. Contains media-specific segment statistics for Ethernet. If you're using RMON2 probes, this table is useful for the RMON domain.

- **Host**. Contains basic host statistics.
- **Conversations**. Contains basic conversations statistics.

Note that the Host group is not a function of mini-RMON and so is supported by the *ForeRunner* ES-3810, but not the PowerHub 6000 or PowerHub 7000 switches unless you have a network probe attached to the network.

#### 9.1.2.1 Viewing Tables

When you want to look at any of the above table types, you can choose the specific type of content that you want. This means that you can look at any of the tables described above for the following types of content:

- **Detail**. Shows a high level (usually hourly) of detail for the table you request as a report.
- **Summary**. Shows a less detailed daily level for the table you request as a report.
- **Snapshot**. Contains temporary information, but report applications do not reference it; only daemons see and work with information in this table.

Trend Reporter uses Detail and Summary tables to extract the information required to prepare various reports you might request.



### 9.1.3 Other Trend Reporter Features

Trend Reporter gives you the flexibility to choose predefined reports through the GUI or to make ad hoc queries to the tables in the database. Other benefits of Trend Reporter that you might be interested in are:

- **Detail and summary data formats**. As mentioned earlier, you can choose to view any of Trend Reporter's seven table types as either detail or summary. This means for any of the seven table types, you can choose the type of content that reflects your organization's current needs, whether it's highly detailed or summary-level information.
- **Automatic data aging**. This feature lets you specify what type of data you want to save in the database for a defined period of time. For example, you might want hourly detail information to stay in the database for seven days, while you'd need daily summary information to stay in the database for a month. Once you specify the amount of time you want to save information, Trend Reporter automatically deletes the aged information.
- **Automatic report generation**. Using Trend Reporter's GUI interface, you can specify that a certain report must be generated on any combination of daily, weekly, and monthly intervals. Once you do so, Trend Reporter schedules the

report to be run at all the intervals you specified. Trend Reporter does this automatic report generation by using an "autoreporter daemon" that you'll read more about later in this chapter.

- **Minimum threshold specification**. This feature lets you specify a minimum utilization percentage for entries to be written to a summary table. You can specify the minimum utilization for a host or a conversation (source-to-destination).

  This means that the Extraction daemon compares a host segment's utilization percentage or source-to-destination utilization percentage to the minimum numbers you specify and creates a row in the host details table only if the utilization percentage meets or exceeds this value. This feature lets you specify what utilization is meaningful to your organization.

## 9.2 Working with Trend Reporter's GUI

When you want to run predefined Trend Reporter reports, you can use the GUI. Reports you can choose to run are defined in Choosing Report Formats and Reports on page 9-17.

Whenever you want to work with Trend Reporter, you need to use the procedure below to display the main window. Once the main window is displayed, you can specify parameters for the aging and logging activities. Use the following procedure to display the Trend Reporter main window.

1. If you haven't already done so, log in to the network management station where *ForeView RMON **ST*** is installed, and run the *ForeView RMON **ST*** application.
2. Select an agent, agent group, or switch from those shown in the list boxes. If the agent you want is *not* listed, you may need to add it. For information about adding agents, see Chapter 4 in this manual.
3. To launch Trend Reporter, click on the Trend Reporter icon or select Application/Trend Reporter from the *ForeView RMON **ST*** main window menu bar, or select Tools/Trend Reporter from within the Domain Manager applications. The Trend Reporter main window, as shown in Figure 9.1, is displayed.

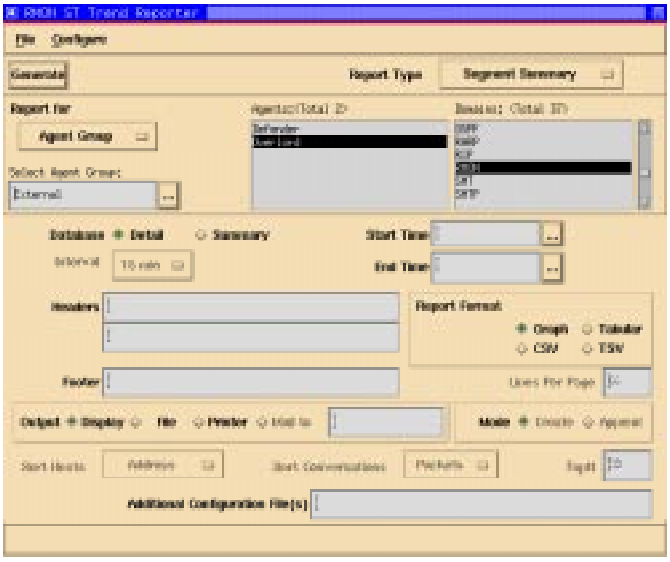



**Figure 9.1 -** Trend Reporter main window

4. From this main window, you can now use Trend Reporter to do the following:
   - **Configure aging parameters**. To do so, see Configuring Aging Parameters on page 9-6.
   - **Configure logging parameters for Poller**. To do so, see Configuring Logging Parameters for Poller on page 9-7.
   - **Generate reports**. To do so, see Generating Predefined Reports with Trend Reporter's GUI on page 9-10.
   - **Create a new or modify an existing report configuration file**. To do so, see Creating and Modifying Report Configuration Files on page 9-12.
   - **Load an existing report configuration file**. To do so, see Loading Existing Report Configuration Files on page 9-14.
   - **Generate reports to run automatically on a scheduled basis**. To do so, see Generating Reports Automatically using Auto Reporter on page 9-14.

## 9.2.1 Configuring Aging Parameters

To specify how long Trend Reporter waits before "aging out" (deleting) data from various tables, you need to configure aging parameters. You also use aging parameters to specify the minimum utilization % required before information is included in the database. To configure the aging parameters you want, use the following procedure.

1. If you haven't already done so, run *ForeView RMON **ST*** and click on the Trend Reporter icon to display the Trend Reporter main window, shown in Figure 9.1 on page 9-5.
2. Select Configure/Aging from the menu bar to access the Configure Aging window, shown in Figure 9.2. You'll notice that there are three headings on this window: **Database, Detail Aging (days)**, and **Summary Aging (days)**. Under the **Database** heading are listed **Protocol, Segment, Host**, and **Conversation**. To the right of each of these table types are two fields—one where you can specify the amount of time to save information in the detail table, and the other where you specify the amount of time to save information in the summary table.


**Figure 9.2 -** Configure Aging window

3. Do the following:
   - To the right of the **Protocol** field, under the **Detail Aging (days)** and **Summary Aging (days)** headings, type a number (greater than 1) in each field to indicate the number of days you want Trend Reporter to wait before it deletes the information in the detail and summary tables.
   - To the right of the **Segment** field, under the **Detail Aging (days)** and **Summary Aging (days)** headings, type a number (greater than 1) in each field to indicate the number of days you want Trend Reporter to wait before it deletes the information in the detail and summary tables.

- To the right of the **Host** field, under the **Detail Aging (days)** and **Summary Aging (days)** headings, type a number (greater than 1) in each field to indicate the number of days you want Trend Reporter to wait before it deletes the information in the detail and summary tables.
- To the right of the **Conversation** field, under the **Detail Aging (days)** and **Summary Aging (days)** headings, type a number (greater than 1) in each field to indicate the number of days you want Trend Reporter to wait before it deletes the information in the detail and summary tables.

4. Under the **Minimum utilization % for inclusion in** heading, do the following:
   - To the right of the **Host Database** field, type the minimum utilization percentage you want.
   - To the right of the **Conversation Database** field, type the minimum utilization percentage you want.
5. To save and apply your choices, click on the Apply button, or to close the window without saving your choices, click on Cancel.



## 9.2.2 Configuring Logging Parameters for Poller

To specify what agents, agent groups, or switches for which you want to log information, you need to configure logging parameters for Trend Reporter's Poller. To do so, use the following procedure. You use this procedure anytime you need to add new logging parameters, edit your existing ones, or delete those you don't need any longer.

1. If you haven't already done so, run *ForeView RMON* ***ST*** and click on the Trend Reporter icon to display the Trend Reporter main window (Figure 9.1 on page 9-5).
2. Select Configure/Poller from the menu bar to access the Configure Poller window. The window is shown in Figure 9.3.

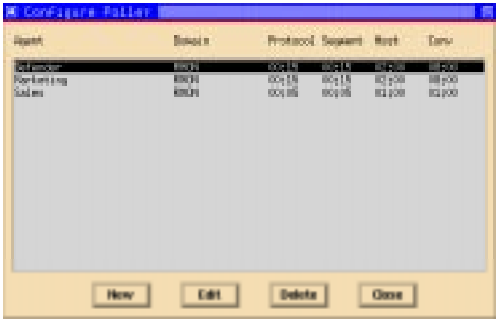



**Figure 9.3 -** Configure Poller window

3. Depending on your situation, do one of the following:
   - **To add a new logging entry**, click on New. The Add Configuration Entry window is displayed, as shown in Figure 9.4.
   - **To edit an existing logging entry**, highlight the entry you want and click on Edit. The Edit Configuration Entry window is displayed.
   - **To delete a logging entry you no longer need**, highlight the entry you want and click on Delete. A dialog is displayed that requires you to confirm that you want to delete the specified entry.
   - **To close the window without making any changes**, click on Close.

NOTE

The New and the Edit windows contain identical fields.

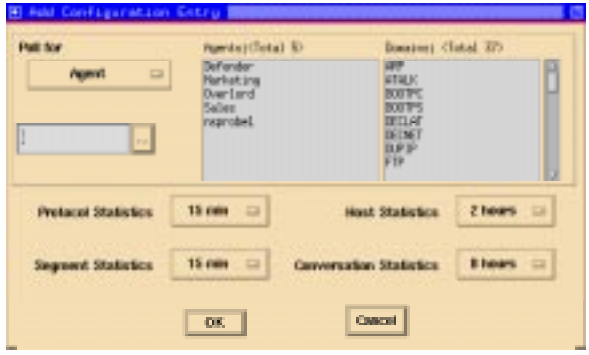



**Figure 9.4 -** Add Configuration Entry window

4. Under the **Poll for** field, click on the selection button and choose either Agent, Agent Group, Switch, or Frame Relay, depending on the device or devices you're setting up to poll information.
5. Do one of the following, depending on your selection in Step 4.
   - **If you selected a single agent**, just find the one you want listed under the **Agents** list box and highlight it.
   - **If you selected an agent group**, click on the selection button under the **Select Agent Group** field. When the Select Agent Group window is displayed, select the group you want and click on OK. Then highlight any combination of agents within that group, shown under the **Agents** list box.

- **If you selected a switch**, click on the selection button under the **Select Switch** field. When the Select Switch window is displayed, select the switch you want and click on OK. Then highlight any combination of ports shown under the **Ports** list box.

NOTE

Depending on your selection, you'll see either the **Select Agent Group** window or the **Select Switch** window. Except for the title bars and the available selections, the windows are the same. The **Select Agent Group** window is shown in Figure 9.5.



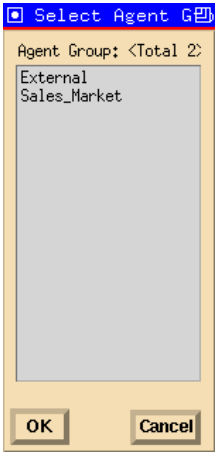



**Figure 9.5 -** Select Agent Group window

6. Highlight one or more domains you want. Depending on how many domains are installed, the list box you see may contain a scroll bar; you can use the scroll bar to see the entire list of domains that are available to be selected for polling information.
7. Do the following:
   - To the right of the **Protocol Statistics** field is a selection button; click on it and select the time interval you want to have protocol statistics collected.
   - To the right of the **Host Statistics** field is a selection button; click on it and select the time interval you want to have host statistics collected.

- To the right of the **Segment Statistics** field is a selection button; click on it and select the time interval you want to have segment statistics collected.
- To the right of the **Conversation Statistics** field is a selection button; click on it and select the time interval you want to have conversation statistics collected.

8. To save and apply your choices, click on the OK button, or to close the window without saving your choices, click on Cancel.

### 9.2.3 Generating Predefined Reports with Trend Reporter's GUI

You can generate many predefined reports from the Trend Reporter main window. Reports you can choose from are defined in Choosing Report Formats and Reports on page 9-17. To generate any of these reports, use the following procedure.

1. If you haven't already done so, run *ForeView RMON **ST*** and click on the Trend Reporter icon to display the Trend Reporter main window (see Figure 9.1 on page 9-5).
2. Select the type of report you want to generate by clicking on the button to the right of the **Report Type** field. Report types you can choose from are described on page 9-18.
3. Under the **Report for** field, click on the selection button and choose either Agent, Agent Group, Switch, or Frame Relay, depending on the device or devices you've set up to poll information that you want generated as a report.
4. Do one of the following, depending on your selection in Step 3.
   - **If you selected a single agent**, just find the one you want listed under the **Agents** list box and highlight it.
   - **If you selected an agent group**, click on the selection button under the **Select Agent Group** field. When the **Select Agent Group** window is displayed, select the group you want and click on OK. Then highlight any combination of agents within that group, shown under the Agents list box.
   - **If you selected a switch**, click on the selection button under the **Select Switch** field. When the **Select Switch** window is displayed, select the switch you want and click on OK. Then highlight any combination of ports shown under the Ports list box.
   - Depending on your selection, you'll see either the **Select Agent Group** window or the **Select Switch** window. Except for the title bars and the available selections, all of the windows are the same. The **Select Agent Group** window shown in Figure 9.5 on page 9-9 gives you an idea of what to expect.
5. Highlight one or more domains you want from those displayed in the **Domains** list box. Depending on how many domains are installed, the list box you see may con-

tain a scroll bar; you can use the scroll bar to see the entire list of domains that are available to be selected for polling information.

6. To the right of the **Database** field, select one of the following buttons:
   - **Detail**, to see highly-detailed content for the report you chose.
   - **Summary**, to see daily summary-level content for the report you chose.
7. To select the total amount of time that you want to see statistics, you need to set a beginning and end date and time. For example, to see statistics for the report you selected for seven days, you might select April 22, 01:00 through April 28, 01:00. To set the total amount of time that you want statistics for, do the following:
   - In the **Start Time** field, click on the selection box to the right of the field; doing so displays a list of dates and times. Highlight the date and time you want the report to start and click on OK.
   - In the **End Time** field, click on the selection box to the right of the field; this displays a list of dates and times. Highlight the date and time you want to designate as the end of the report and click on OK. The time you select in this field *must* be a later date and time than what you selected in the **Start Time** field.
8. In the **Interval** field, click on the selection box to select the time interval you want reflected in the report you chose. For example, if you want to see information collected every hour, you'd select 1 hour as the interval.
9. To print headers and footers on the report, do the following:
   - To print information at the top of the report, enter up to two lines of information (up to 80 printable characters) in the Headers field.
   - To print information at the bottom of the report, enter one line of information (up to 80 printable characters) in the **Footers** field.
10. In the Report Format field, click on the button by the format type you want for the selected report. You can choose from Graph, Tabular, CSV, and TSV. Keep in mind that not all types are available for all reports. For more about the types you can choose, see Choosing Report Formats and Reports on page 9-17.
11. In the **Lines Per Page** field, enter the total number of text lines you want on each page of a Tabular report. If you selected any other report format (Graph, CSV, or TSV), this option is dimmed.
12. To choose the output of your report, choose from one of the following buttons shown to the right of the Output field:
    - **Display**. Report is shown on the management console's screen. From this screen, you can print it to a printer or file, as explained on page 9-16. Go to Step 14.

- **File**. Report is saved as a file. You must specify a new or existing file in the blank field shown to the right of the available output options. When you choose this option, you must also click either the Create (to create a new file) or Append (to add the report to an existing file) button. Go to Step 13.
- **Printer**. Report is queued directly to a printer. You must specify the printer name in the blank field shown to the right of the available output options. Go to Step 14.
- **Mail to**. Report is sent as an email message. You must specify the email address in the blank field shown to the right of the available output options. Go to Step 14.

13. If you selected a file output, in the **Mode** field, you must also click either the Create (to create a new file) or Append (to add the report to an existing file) button.
14. If you've selected a Host-type report, in the **Sort Hosts** field, click on the selection button to the right of the field to select the variable you want; the report is sorted using this variable. If you selected any report type other than Host, this option is dimmed. You can choose from Address, Packets, Packets-in, Packets-out, Utilization, Utilization-in, or Utilization-out.
15. If you've selected a Conversations-type report, do the following to set up the report:
    - In the **Sort Conversations** field, click on the selection button to the right of the field to select the variable you want; the report is sorted using this variable. If you selected any report type other than Conversation, this option is dimmed. You can choose from Packets or Utilization.
    - In the **Top N** field, enter the number that reflects how many of the highest traffic conversations you want to see. The conversations you'll see on the report are based on this number and on the variable you select in the **Sort Conversations** field. If you selected any report type other than Conversation, this option is dimmed.
16. In the **Additional Configuration File(s)** field, specify any additional configuration files you want Trend Reporter to use when generating the report.
17. To generate the report as specified, click on the Generate button, displayed at the top of the Trend Reporter main window (Figure 9.1 on page 9-5).

### 9.2.3.1 Creating and Modifying Report Configuration Files

When you fill out the Trend Reporter main window to generate a report, you're also configuring the report; you can save the configuration and use it again.

You'd want to save a report configuration in a file if it produces a report that you like the looks of, but maybe don't run it often enough to set it up with the AutoReporter. Or, if you're asked to quickly run each type of available report for a specific time period for comparison pur-

poses, you can set up and save one configuration file and just modify it as required for each report. Doing so saves you the time it takes to configure all the variables for each report offered in Trend Reporter.

Don't confuse this with configuring logging or aging parameters—those tasks let you specify what statistics are reported, and when collected statistics are deleted from the database, respectively.

The report configuration file is just a collection of variables that impact what report you generate, where (and to what) the report is output, what time the report begins and ends, specific headers or footers, and whether the report is in graph, tabular, CSV or TSV format, among other things. Use the procedure below to create or modify report configuration files.



1. If you haven't already done so, display the Trend Reporter main window (for steps on doing this, see Working with Trend Reporter's GUI on page 9-4).
2. Fill out or modify the fields on this window as described beginning on page 9-10, starting with Step 2.
3. Before clicking the Generate button to actually run the report, do the following:
   - **If you're creating a new report configuration file**, select File/Save.
     *or*
   - **If you're modifying an existing report configuration file**, select File/Save As. The Enter file name window shown in Figure 9.6 is displayed.


**Figure 9.6 -** Enter file name window

4. In the **Selection** field at the bottom of the window, type the name you want for the report configuration file and click on OK. One of the following occurs:
   - **If you chose** File/Save, the new file is saved in the directory displayed in the Filter field, under the name you assigned. Keep in mind that if you mistakenly choose File/Save when you're editing a report configuration file, the

changes you make overwrite the old report configuration file. This is why we recommend selecting File/Save As for editing existing files.
*or*

- **If you chose** File/Save As, the changes you made to the existing file are saved in the new filename you specified. The existing file you used as a template is not changed.

## 9.2.4 Loading Existing Report Configuration Files

Whenever you want to use an existing report configuration file to control how a report should look, as well as the report time interval, among other variables, you can load an existing report configuration file. Loading an existing report configuration file saves you the work of filling out all the fields on the Trend Reporter main window. This is especially useful when you need to generate a report fast. Use the following procedure to load an existing file.

1. If you haven't already done so, display the Trend Reporter main window (for steps on doing this, see Working with Trend Reporter's GUI on page 9-4).
2. Select the type of report you want to generate by clicking on the button to the right of the **Report Type** field. Report types you can choose from are described in About Predefined Reports on page 9-18.
3. Select File/Load from the menu bar to display the Enter file name window. The Enter file name window is shown in Figure 9.6 on page 9-13.
4. Locate and highlight the name of the report configuration file you want to load. To do so, use the scroll bars in the **Directories** and **Files** list boxes as necessary, then click on OK. The remaining fields on the Trend Reporter main window are filled in with the values specified in the report configuration file you loaded.
5. To generate the report you selected with the parameters loaded from the specified report configuration file, click on Generate.

## 9.2.5 Generating Reports Automatically using Auto Reporter

To save you time, Trend Reporter offers the Auto Reporter feature. Auto Reporter lets you schedule reports to run on a daily, weekly, or monthly basis. This is particularly useful if you've set up certain reports that you need on a regular basis. Once you define the reports you want to run through Auto Reporter, it takes care of all the rest, and provides the reports as you specify. To set up reports to run regularly in Auto Reporter, use the following procedure.

1. If you haven't already done so, display the Trend Reporter main window (for steps on doing this, see Working with Trend Reporter's GUI on page 9-4).
2. From the menu bar, select Configure/Auto Reporter. The Configure Auto Reporter window as shown in Figure 9.7 on page 9-15 is displayed.


Keep in mind that the Configure Auto Reporter window shown in Figure 9.7 is blank. This is how the window looks when you first access it. Later, after you've scheduled regular reports, each one is represented by a separate line that indicates how it's scheduled.


**Figure 9.7 -** Configure Auto Reporter window

3. Click on the **New** button to display the Add Configuration Entry window. This window is shown in Figure 9.8.


**Figure 9.8 -** Add Configuration Entry window

4. Under the **Generate Report Automatically** heading, click on either the Daily, Weekly, or Monthly button.
5. In the **Configuration File** field, enter the name of the configuration file containing the parameters and variables you've defined for the report you're scheduling. Or, click on the selection button to the right of the field to browse through available report configuration files so you can make your choice.
6. Click on Apply to set the report to run as scheduled, or click on Cancel to close the window without saving the information.

### 9.2.6 Editing Reports Scheduled in Auto Reporter

It's easy to reschedule reports in Auto Reporter. To do so, use the following procedure.

1. If you haven't already done so, display the Trend Reporter main window (for steps on doing this, see Working with Trend Reporter's GUI on page 9-4).
2. From the menu bar, select Configure/Auto Reporter. The Configure Auto Reporter window shown in Figure 9.7 on page 9-15 is displayed.
3. Click on the Edit button. The Edit Configuration Entry window is displayed. The fields on the window are identical to the Add Configuration Entry window shown in Figure 9.8 on page 9-15.
4. In the **Configuration File** field, enter the name of the configuration file containing the parameters and variables defined for the report you're rescheduling. Or, click on the selection button to the right of the field to browse through available report configuration files so you can make your choice.
5. Under the **Generate Report Automatically** heading, reschedule the report by clicking on either the Daily, Weekly, or Monthly button.
6. Click on Apply to set the report to run on the new scheduled basis, or click on Cancel to close the window without saving the change.

### 9.2.7 Printing GUI-Generated Reports

Use the following procedure to print any report you've generated through the Trend Reporter GUI and displayed on the network management console screen.


You can print a report to a file, directly to a printer, or send the report as an email. For more information, see page 9-11.

1. With the report displayed on screen, select File/Print from the menu bar to open the Print Options window displayed in Figure 9.9 on page 9-17.


**Figure 9.9 -** Print Options window

2. Do one of the following:
   - To print the report to a file, select **File** as the destination, specify the directory path under **Directory**, and type the filename in the **File** field.
     *or*
   - To print the report directly to a printer, select **Printer** as the destination, and type the printer name in the **Printer** field.
3. Click on Apply.

## 9.3 Choosing Report Formats and Reports

Trend Reporter features various reports that you can choose from, depending on your organization's needs. The table below shows all the reports you can run, as well as types of formats you can choose for each.

| This report: | Is available in these formats: |
|---|---|
| Segment Summary | Tabular, Graphical, CSV, TSV |
| Segment Details | Graphical, CSV, TSV |
| Host Summary | Tabular, Graphical, CSV, TSV |
| Host Verbose | Tabular, CSV, TSV |
| Host Outbound | Tabular, CSV, TSV |
| Conversation Summary | Tabular, Graphical, CSV, TSV |

| This report: | Is available in these formats: |
|---|---|
| Billing | Tabular, CSV, TSV |
| Multi Segment Summary | Tabular, Graphical, CSV, TSV |
| Host Details | Tabular, Graphical, CSV, TSV |
| Conversation Details | Tabular, Graphical, CSV, TSV |
| VLAN Usage | Tabular, Graphical, CSV, TSV |

### 9.3.1 About Predefined Reports

Each predefined report gives you specific information. Use the table below to decide what types of reports you might want to generate.

| This report: | For the interval you specify, provides: |
|---|---|
| Segment Summary | a summary of segment traffic. |
| Segment Details | details of all segment traffic. |
| Multi-Segment Summary | information about segments for a specified agent group or switch. |
| VLAN Usage | information about traffic on all VLANs associated with the monitored Fast Ethernet segment. |
| Router Backbone Usage | information about traffic on all nodes connected to the specified router backbone. |
| Host Summary | a summary of host traffic, sorted as you specify. You can choose to include just one host or the Top N Hosts. |
| Host Verbose | details of host traffic, sorted as you specify. You can choose to include just one host or the Top N Hosts. |
| Host Outbound | details of all outbound host traffic, sorted as you specify. You can choose to include just one host or the Top N Hosts. |
| Host Details | details of host traffic, sorted as you specify. You can choose to include just one host or the Top N Hosts. |

| This report: | For the interval you specify, provides: |
|---|---|
| Conversation Summary | a summary of traffic between each pair of hosts that has "talked." |
| Conversation Details | a detail of traffic between each pair of hosts that has "talked." |

NOTE

Only the Segment Summary, Segment Details, and Multi-Segment Summary reports are supported by mini-RMON. The others are available on the *ForeRunner* ES-3810.



### 9.3.2 About Report Formats

Depending on the report you select, you can usually choose from several different report formats. Here's what to expect from the different report formats:

- **Tabular**. Information is displayed as alphanumeric and numeric text in columns and rows. Typically, you'd want to select this format when you're using the information as a standalone report.
- **Graphical**. Information is displayed in graph format with a corresponding legend. Typically, you'd want to select this format when you're using the information as a standalone report.
- **CSV** (Comma Separated Value). Information is displayed as alphanumeric and numeric text in strings, with values separated by commas. Typically, you'd want to select this format when you plan to import the information into a spreadsheet type application.
- **TSV** (Tab Separated Value). Information is displayed as alphanumeric and numeric text in strings, with values separated by a tab character. Typically, you'd want to select this format when you plan to import the information into a spreadsheet type application.

## 9.4 How Trend Reporter's Database Works

Trend Reporter uses a single database, named NSTREND_DB, that contains all *ForeView RMON **ST***-related tables. There are many tables in this database that Trend Reporter accesses in response to choices you make on the GUI, or to ad hoc SQL queries you enter. Other *ForeView RMON **ST*** applications may also access some of the tables in the database.

Within the database, you'll find sets of tables and types of tables. What's the difference? There

are several types of tables (described in More About Trend Reporter's Database Tables on page 9-2); for each type of table, three storage tables exist. (For more details about the storage tables and how the daemons work with the information contained in each, see Chapter 10.) The three storage tables, and how they work, are explained as follows:

- **Snapshot**. These tables contain raw snapshot data. The snapshot daemon creates each new row in the snapshot table.
- **Details**. These tables are created using information from the Snapshot tables, and offer high-granularity time resolution, meaning statistics for small, meaningful timeframes. The database extraction daemon gets the raw information from the Snapshot table in pairs of rows, calculates the difference between the two rows, and stores the difference in the Details table.
- **Summary**. These tables are created from the Detail tables and offer 24-hour granularity only, meaning statistics summarized over a 24-hour period. The database rollup daemon is responsible for creating this table by pulling out 24 hours of information from the Details table, and summarizing the statistics to compare with older 24-hour periods. The information in this table, except for the longer timeframe, is identical to the corresponding Details table.

### 9.4.1 Database Table Quick Reference

For more detail about these tables, see Working with Trend Reporter's GUI on page 9-4. Some tables in the section combine detail and summary information. For quick reference, the table below shows a list of all the tables in the database and gives a brief description of each as well as maximum row size.

| Table name | Description | Maximum row size |
|---|---|---|
| seg_et_snap | Ethernet segment statistics snapshots | 260 |
| seg_et_detail | Ethernet segment statistics details | 280 |
| set_et_summary | Ethernet segment statistics summary | 280 |
| seg_tr_detail | Token Ring segment statistics details | 469 |
| seg_tr_summary | Token Ring segment statistics summary | 469 |
| host_snap | Host statistics snapshots | 205 |
| host_detail | Host statistics details | 225 |
| host_summary | Host statistics summary | 225 |
| conv_snap | Conversation statistics snapshots | 181 |
| conv_detail | Conversation statistics details | 201 |
| conv_summary | Conversation statistics summary | 201 |

## 9.4.2 Understanding Trend Reporter's Daemons

As you might know, a daemon is a UNIX process that runs in the background and is disconnected from a process group and terminal. As used in Trend Reporter, certain daemons are used to update functions. Daemons work with related configuration files that control how and when they are called to perform their roles. Daemons used in Trend Reporter are:

- **Snapshot daemon**. Called `dbsnapd`, this daemon gets snapshots of raw statistics from agents and stores this information in a snapshot table.
- **Extraction daemon**. Called `dbextrad`, this daemon gets information from the snapshot table, creates new rows in the details table, and deletes the oldest member in each pair of snapshot rows.
- **Rollup & Aging daemon**. Called `dbrolld`, this daemon performs two separate-but-related actions; it gets information from the details table to create new rows in the summary table, and deletes obsolete information from both the detail and summary tables.
- **Server daemon**. Called `msqld`, this daemon is bundled with the SQL server and listens and processes SQL queries (direct or those from the GUI).

# CHAPTER 10 Customizing Trend Reporter

Trend Reporter is based on a relational database, which means that you can make ad hoc queries to information contained in any of the database's tables, set up automatic report generation, choose reports based on detail or summary data, and define how long detail or summary information stays in the database. Trend Reporter includes a bundled Structured Language Query (SQL) server.

This chapter contains a brief overview of Trend Reporter, an in-depth discussion of Trend Reporter's daemons, details about the different tables, information about the table schemata, information about setting up environment variables, administering the database, and using SQL queries to generate customized, ad hoc reports.

If you are not already familiar with Trend Reporter or SQL, please see How Trend Reporter Works on page 9-1 before continuing in this chapter.

The following sections contain more detailed information on Trend Reporter and how to customize the application:

# 10.1 Understanding the Reporting Features

In Trend Reporter, you can generate reports two ways: interactively, through the GUI, or on an ad hoc basis, using SQL queries. Depending on your needs, you might need to run the predefined reports, create your own ad hoc reports, or a combination of some predefined reports with some ad hoc reports you customize.

## 10.1.1 About Report Formats

Depending on the report you select, you can usually choose from several different report formats. The formats are Tabular, Graphical, CSV, and TSV and defined in Chapter 9.

# 10.2 Behind the Scenes: What's in the Database

Trend Reporter uses a single database, named NSTREND_DB, that contains all *ForeView RMON **ST***-related tables. As you might guess, Trend Reporter accesses many tables in this database in response to choices you make on the GUI, or to ad hoc SQL queries you enter. Other *ForeView RMON **ST*** applications may also access some of the tables in the database.

Within the database, you'll find sets of tables and types of tables. What's the difference? There are seven types of tables (described in More About Trend Reporter's Database Tables on page 9-2); for each type of table, three storage tables exist. The three storage tables, and how they work, are explained as follows:

- **Snapshot**. These tables contain raw snapshot data. The snapshot daemon creates each new row in the snapshot table. The database extraction daemon uses each available pair of rows in the snapshot table to create a corresponding row in the detail table. Once the database extraction daemon uses a pair of rows, the older row is discarded, and the second row (the newer one) becomes the older row once new data is received and logged. Trend Reporter just uses this type of table as a resource to produce usable statistics for the Detail and Summary tables.
- **Details**. These tables are created using information from the Snapshot tables, and offer high-granularity time resolution, meaning statistics for small, meaningful timeframes. The database extraction daemon gets the raw information from the Snapshot table in pairs of rows, calculates the difference between the two rows, and stores that in the Details table. Once the database extraction daemon is finished calculating, the information's ready to use. You can request specific detail tables, either through Trend Reporter's GUI, or on an ad hoc basis, using specific SQL queries.

- **Summary**. These tables are created from the Detail tables and offer 24-hour granularity only, meaning statistics summarized over a 24-hour period. The database rollup daemon is responsible for creating this table by pulling out 24 hours of information from the Details table, and summarizing the statistics to compare with older 24-hour periods. The information in this table, except for the longer timeframe, is identical to the corresponding Details table. Depending on how you use the summary information and your organization's needs, you might specify the database aging daemon to delete older rows from the Summary table once a week, or whenever you consider summary information to be obsolete.



## 10.2.1 Database Table Quick Reference

For quick reference, the table below shows a list of all the tables in the database, gives a brief description of each, as well as maximum row size.

| Table name | Description | Maximum row size |
|---|---|---|
| seg_et_snap | Ethernet segment statistics snapshots | 260 |
| seg_et_detail | Ethernet segment statistics details | 280 |
| set_et_summary | Ethernet segment statistics summary | 280 |
| host_snap | Host statistics snapshots | 205 |
| host_detail | Host statistics details | 225 |
| host_summary | Host statistics summary | 225 |
| conv_snap | Conversation statistics snapshots | 181 |
| conv_detail | Conversation statistics details | 201 |
| conv_summary | Conversation statistics summary | 201 |


To see even more detail about all of these tables, go to Understanding Trend Reporter's Table Schemata on page 10-9. In that section, be aware that some tables combine detail and summary information.

## 10.2.2 Understanding Trend Reporter's Daemons

As you might know, a daemon is a UNIX process that runs in the background and is disconnected from a process group and terminal. As used in Trend Reporter, certain daemons are used to update functions. Daemons work with related configuration files that rule how and when they are called to perform their roles. Daemons used in Trend Reporter are:

- **Snapshot daemon**. Called dbsnapd, this daemon gets snapshots of raw statistics from agents and stores this information in a snapshot table.
- **Extraction daemon**. Called dbextrad, this daemon gets information from the snapshot table, creates new rows in the details table, and deletes the oldest member in each pair of snapshot rows.
- **Rollup and Aging daemon**. Called dbrolld, this daemon performs two separate-but-related actions; it gets information from the details table to create new rows in the summary table, and deletes obsolete information from both the detail and summary tables.
- **Server daemon**. Called msqld, this daemon is bundled with the SQL server and listens and processes SQL queries (direct or those from the GUI).

### 10.2.2.1 More About the Snapshot Daemon

The Snapshot daemon, dbsnapd, creates logs based on specifications in the $NSHOME/usr/dbsnap.cfg configuration file. The Snapshot daemon creates rows in snapshot tables, rather than individual logfiles.

### 10.2.2.2 How the Snapshot Daemon Works with the dbsnap.cfg File

The ASCII configuration file, dbsnap.cfg, contains information that controls how the Snapshot daemon works. In this file are the agent/domain combinations you want to log, as well as snapshot intervals that the daemon uses to gather raw data.


The Snapshot daemon gathers information **only** for the agent/domain combinations that are specified in the dbsnap.cfg file.

The smallest selectable interval is one minute (although you can specify a different interval, depending on your needs). For example, you'd probably want to use the small one minute interval when you want to log protocol and segment statistics.

The Snapshot daemon reads the dbsnap.cfg file at the start of every defined interval, so that any changes to the file are effective for the next logging interval. For example, if you specify 04:00 as a logging interval, Trend Reporter takes snapshots at 4 a.m., 8 a.m., 12 noon, and so on. Logging intervals you can specify in the dbsnap.cfg file are:

- - (dash, which indicates no logging at all)
- 00:01 (log every minute)
- 00:05 (log every five minutes)
- 00:15 (log every 15 minutes)
- 00:30 (log every 30 minutes)
- 01:00 (log every hour)
- 02:00 (log every two hours)
- 04:00 (log every four hours)
- 08:00 (log every eight hours)
- 24:00 (log every 24 hours)



Each line in the dbsnap.cfg file contains an agent name, domain name, and interval to log for protocol, segment, host, and conversation information. The sample below is similar to the contents of your dbsnap.cfg file.

```
#Agent Domain   Protocol   Segment   Host     Conversation

et1_05 RMON     00:05      00:05     00:30    24:00

et2_05 RMON     00:05      -         02:00    24:00

et3_32 RMON     00:05      01:00     02:00    08:00

et4__32RMON     00:05      -         02:00    04:00
```

Using the example above, for agent et4_32 and domain RMON, Trend Reporter would log conversation statistics starting at midnight, and again at 4:00 a.m., 8:00 a.m., 12:00 p.m. (noon), 4:00 p.m., and 8:00 p.m. This means that every four hours (04:00), Trend Reporter takes a snapshot of the conversation statistics for agent et4_32.

NOTE

The sample dbsnap.cfg layout shown above is almost identical to the GUI. For more about selecting logging intervals, see Configuring Logging Parameters on page 10-18.

#### 10.2.2.3 More About the Extraction Daemon

The Extraction daemon, dbextrad, "follows" the Snapshot daemon, and creates entries in the detail tables derived from the snapshot pairs in snapshot tables. Whenever the Extraction daemon uses a pair of rows in the snapshot table, it also deletes the older row, since that snapshot information is no longer needed.

The Extraction daemon ignores snapshots taken more than 24 hours apart. After the Extraction daemon goes through a snapshot table, it deletes snapshots older than 48 hours; this is especially useful to delete snapshots for agent / domain combinations that no longer have logging enabled.

### 10.2.3 How the Extraction, Rollup and Aging Daemons Work with the dbupdate.cfg File

The ASCII configuration file, dbupdate.cfg, contains information that controls how the Extraction and Rollup and Aging daemons work. In this file are parameters you can customize as necessary. Remember, you can't delete any of the tables in the database (they're permanent), but you can specify that old rows of information be deleted at specific intervals.

In the dbupdate.cfg file, you'll find one line of information and parameters (shown in number of days) for each type of table (protocol, segment, host, and conversation). Also in the file are minimum utilization thresholds for the host and conversation tables only. The sample below is similar to the contents of your dbupdate.cfg file.

```
#                    Detail Aging   Summary Aging

Protocol:                    31             366
Segment:                     31             366
Host:                         7              31
Conversation:                 7              31
#
#Minimum utilization percentage for inclusion in host
#and conversation detail/summary tables
HostThreshold:                        0.010
ConversationThreshold:                0.005
```

NOTE

The sample dbupdate.cfg layout in the above example is almost identical to the GUI. For more about selecting aging parameters, see Configuring Report Parameters on page 10-18.

In this configuration file, there are only four parameters you can modify, as explained below:

- **Detail Aging**. This interval shows the number of days that information can age before the Rollup and Aging daemon deletes it from the details table. Using the example above, for a host details table, information is allowed to age for seven days and then it's deleted from that table. You must specify a value greater than 1.
- **Summary Aging**. This interval shows the number of days that information can age before the Rollup and Aging daemon deletes it from the summary table. Using the example above, for a protocol summary table, information is allowed to age for 366 days and then it's deleted from that table. You must specify a value greater than 1.
- **HostThreshold**. This number shows the minimum utilization percentage that a host inbound and outbound must meet before it's included in the host details or summary tables. This means that the Extraction daemon compares a host segment's utilization percentage to this number and creates a row in the host details table only if the utilization percentage meets or exceeds this value. This is a useful feature that lets you save disk space by saving only certain information that meets the percentage you select.
- **ConversationThreshold**. This number shows the minimum source-to- destination utilization percentage that a conversation must meet before it's included in the conversation details or summary tables. This means that the Extraction daemon compares a conversation's source-to-destination utilization percentage to this number and creates a row in the conversation details table only if the utilization percentage meets or exceeds this value. This is a useful feature that, as part of Trend Reporter's GUI, lets you save disk space by saving only certain information that meets the percentage you select.



## 10.2.4 More About the Rollup and Aging Daemon

The Rollup and Aging daemon, dbrolld, "wakes up" daily at 1:45 a.m. (the default setting). Once it's awake, it uses information in the details tables to create entries in the corresponding summary tables for the previous day. For example, if you've defined hourly protocol logging for the agent named et4_32 for domain RMON, the Rollup and Aging daemon looks at all 24 rows in the protocol detail table, summarizes the information into one row, and puts this summary row in the protocol summary table. The daemon does not delete the 24 rows in the protocol detail table at this point.

Once the Rollup and Aging daemon has looked through all the details tables, and extracted the information to put into the summary tables, it performs an "aging pass." This aging pass is when the daemon goes through both details and summary tables looking for old information that has aged past the limits set in the dbupdate.cfg file. When the Rollup and Aging daemon finds information that's aged past the limits, it deletes it. (For more about the dbupdate.cfg file, see page 10-6.)

## 10.2.5 More About the Server "Daemon"

The Server "daemon", msqld, is really a server process that acts like, but is not technically a daemon (although for ease of use, we call it that in this book). The Server daemon is bundled with *ForeView RMON **ST*** on Motif platforms. When you start *ForeView RMON **ST***, this wakes up the Snapshot daemon, which then wakes up the Server daemon.

The Server daemon's job is basically to listen for SQL or database administration queries by using either a TCP/IP or a UNIX socket (although currently, connections must be local). The other action-oriented daemons (Snapshot, Extraction, and Rollup and Aging) are now able to connect to the database through the socket that the Server daemon uses.

Keep in mind that, as mentioned earlier, the Server "daemon" is really a server process, and there are no configuration or log files you need to monitor or use, as you might for other daemons.

## 10.2.6 Understanding Daemon Log and Control Files

All of Trend Reporter's true daemons (Snapshot, Extraction, and Rollup and Aging) record their activities by putting their information into log files. Control files are special files that contain code for the "keep alive" mechanism that helps *ForeView RMON **ST*** ensure that exactly one copy of each daemon is running at a given time. The server daemon, msqld, does not log its activity.

We recommend that you occasionally check the daemons' logfiles to ensure that the daemons are functioning correctly. To do so, you can use the **tail-f** UNIX command. Below is a listing of the logfiles you'll want to monitor.

| This daemon | Creates this logfile: | And this control file: |
|---|---|---|
| dbsnapd | dbsnap.log | dbsnap.ctl |
| dbextrad | dbextra.log | dbextra.ctl |
| dbrolld | dbroll.log | no control file is created |

# 10.3 Understanding Trend Reporter's Table Schemata

The following are all the table schemata used in Trend Reporter.

- Segment Snapshot Table (Ethernet-Specific). See page 10-10.
- Host Snapshot Table. See page 10-12.
- Conversation Snapshot Table. See page 10-13.
- Segment Detail and Summary Tables (Ethernet-Specific). See page 10-14.
- Host Detail and Summary Tables. See page 10-16.
- Conversation Detail and Summary Tables. See page 10-17.



## 10.3.1 Protocol Snapshot Table (Media-Independent)

| Field | Type | Description |
|---|---|---|
| Agent | char(26) | Agent name. |
| Domain | char(15) | Domain name. |
| TargetSnapTime | int | Target snapshot time. The actual snapshot may be taken after the target time. |
| TargetSnapTimeText | char(15) | Target snapshot time (text format). |
| ActualSnapTime | int | Actual snapshot time. |
| InstallTime | int | RMON table installation time (or 0 if unavailable). Used to detect domain re-installation. |
| IfSpeed | int | Agent interface speed in bits per second. |
| NetType | char(4) | Agent network type: ET, TR, FDDI, or WAN. |
| SysUpTime | int | Agent SysUpTime at time of snapshot; used to detect domain re-installation. |
| DomainId | int | Domain index. Used to detect domain re-installation. |
| Filler1 | int | Reserved for future use. |
| Octets | real | Value of octets counter at snaphot time. |
| Pkts | real | Value of packets counter at snaphot time |
| Filler2 | real | Reserved for future use. |
| Filler3 | real | Reserved for future use. |

## 10.3.2 Segment Snapshot Table (Ethernet-Specific)

| Field | Type | Description |
|---|---|---|
| Agent | char(26) | Agent name. |
| Domain | char(15) | Domain name. |
| TargetSnapTime | int | Target snapshot time. The actual snapshot may be taken after the target time. |
| TargetSnapTimeText | char(15) | Target snapshot time (text format). |
| ActualSnapTime | int | Actual snapshot time. |
| InstallTime | int | RMON table installation time (or 0 if unavailable). Used to detect domain re-installation. |
| IfSpeed | int | Agent interface speed in bits per second. |
| NetType | char(4) | Agent network type: ET, TR, FDDI, or WAN. |
| SysUpTime | int | Agent SysUpTime at time of snapshot; used to detect domain re-installation. |
| DomainId | int | Domain index. Used to detect domain re-installation. |
| Filler1 | int | Reserved for future use. |
| DropEvents | real | Drop events. This and remaining fields are absolute values of corresponding RMON counters at the time of the snapshot. |
| Octets | real | Total number of Octets received on the network at the time of the snapshot. |
| Pkts | real | The number of Packets received at the time of the snapshot. |
| BroadcastPkts | real | The total number of good packets that were directed to the broadcast address received at the time of the snapshot. |
| MulticastPkts | real | The total number of good packets that were directed to the multicast address received at the time of the snapshot. |
| CRCErrors | real | The number of packets that had a bad FCS with an FCS error, or a bad FCS with an Alignment error at the time of the snapshot. |

| Field | Type | Description |
|---|---|---|
| UndersizePkts | real | The number of UndersizePkts that were less than 64 octets long received at the time of the snapshot. |
| OversizePkts | real | The number of packets longer than 1518 octets received at the time of the snapshot. |
| Fragments | real | The number of Fragments that were less than 64 octets in length and had FCS errors or Alignment errors received at the time of the snapshot. |
| Jabbers | real | The number of Fragments that were longer than 1518 octets in length and had FCS errors or Alignment errors received at the time of the snapshot. |
| Collisions | real | The number of Collisions received at the time of the snapshot (best estimate). |
| Pkts64 | real | The number of packets that were 64 octets in length received at the time of the snapshot. |
| Pkts65to127 | real | The number of packets between 65 and 127 octets in length received at the time of the snapshot. |
| Pkts128to255 | real | The number of packets between 128 and 255 octets in length received at the time of the snapshot. |
| Pkts256to511 | real | The number of packets between 256 and 511 octets in length received at the time of the snapshot. |
| Pkts512to1023 | real | The number of packets between 512 and 1023 octets in length received at the time of the snapshot. |
| Pkts1024to1518 | real | The number of packets between 1024 and 1518 octets in length received at the time of the snapshot. |
| Filler2 | real | Reserved for future use. |
| Filler3 | real | Reserved for future use. |

## 10.3.3 Host Snapshot Table

| Field | Type | Description |
|---|---|---|
| Agent | char(26) | Agent name. |
| Domain | char(15) | Domain name. |
| TargetSnapTime | int | Target snapshot time. The actual snapshot may be taken after the target time. |
| TargetSnapTimeText | char(15) | Target snapshot time (text format). |
| ActualSnapTime | int | Actual snapshot time. |
| InstallTime | int | RMON table installation time (or 0 if unavailable). For detect domain re-installation. |
| IfSpeed | int | Agent interface speed in bits per second. |
| NetType | char(4) | Agent network type: ET, TR, FDDI, or WAN. |
| SysUpTime | int | Agent SysUpTime at time of snapshot; used to detect domain re-installation. |
| DomainId | int | Domain index. For detect domain re-installation. |
| Filler1 | int | Reserved for future use. |
| AddressType | char(4) | Host address type. |
| Address | char(20) | Host address, hex-ASCII format. |
| InPkts | real | Packets in. This and remaining fields are absolute values of corresponding RMON counters at the time of the snapshot. |
| OutPkts | real | Packets out. |
| InOctets | real | Octets in. |
| OutOctets | real | Octets out. |
| OutErrors | real | Errors out. |
| OutBroadcastPkts | real | Broadcast packets out. |
| OutMulticastPkts | real | Multicast packets out. |
| OutNonUcastPkts | real | Non-unicast packets out. |
| Filler2 | real | Reserved for future use. |
| Filler3 | real | Reserved for future use. |

## 10.3.4 Conversation Snapshot Table

| Field | Type | Description |
|---|---|---|
| Agent | char(26) | Agent name. |
| Domain | char(15) | Domain name. |
| TargetSnapTime | int | Target snapshot time. The actual snapshot may be taken after the target time. |
| TargetSnapTimeText | char(15) | Target snapshot time (text format). |
| ActualSnapTime | int | Actual snapshot time. |
| InstallTime | int | RMON table installation time (or 0 if unavailable). Used to detect domain re-installation. |
| IfSpeed | int | Agent interface speed in bits per second. |
| NetType | char(4) | Agent network type: ET, TR, FDDI, or WAN. |
| SysUpTime | int | Agent SysUpTime at time of snapshot; used to detect domain re-installation. |
| DomainId | int | Domain index. Used to detect domain re-installation. |
| Filler1 | int | Reserved for future use. |
| AddressType | char(4) | Host address type. |
| SrcAddress | char(20) | Source host address, hex-ASCII format. |
| DstAddress | char(20) | Destination host address, hex-ASCII format. |
| Pkts | real | Packets source host to destination host. This and remaining fields are absolute values of corresponding RMON counters at the time of the snapshot. |
| Octets | real | Octets source host to destination host. |
| Errors | real | Errors source host to destination host. |
| Filler2 | real | Reserved for future use. |
| Filler3 | real | Reserved for future use. |

## 10.3.5 Segment Detail and Summary Tables (Ethernet-Specific)

| Field | Type | Description |
|---|---|---|
| Agent | char(26) | Agent name. |
| Domain | char(15) | Domain name. |
| StartTime | int | Start time. |
| EndTime | int | End time. |
| StartTimeText | char(15) | Start time (text format). |
| EndTimeText | char(15) | End time (text format). |
| Duration | int | Actual duration of interval in seconds. |
| IfSpeed | int | Agent interface speed in bits per second. |
| NetType | char(4) | Agent network type: ET, TR, FDDI, or WAN. |
| Reinstalled | int | Reinstalled flag, non-zero if reinstalled. |
| Filler1 | int | Reserved for future use. |
| Utilization | real | Average segment utilization for the time interval. |
| DropEvents | real | The “delta” value for the corresponding RMON counter during the interval. |
| Octets | real | The “delta” value for the corresponding RMON counter during the interval. |
| Pkts | real | The “delta” value for the corresponding RMON counter during the interval. |
| BroadcastPkts | real | The “delta” value for the corresponding RMON counter during the interval. |
| MulticastPkts | real | The “delta” value for the corresponding RMON counter during the interval. |
| CRCAlignErrors | real | The “delta” value for the corresponding RMON counter during the interval. |
| UndersizePkts | real | The “delta” value for the corresponding RMON counter during the interval. |
| OversizePkts | real | The “delta” value for the corresponding RMON counter during the interval. |

| Field | Type | Description |
|---|---|---|
| Fragments | real | The “delta” value for the corresponding RMON counter during the interval. |
| Jabbers | real | The “delta” value for the corresponding RMON counter during the interval. |
| Collisions | real | The “delta” value for the corresponding RMON counter during the interval. |
| Pkts64 | real | The “delta” value for the corresponding RMON counter during the interval. |
| Pkts65to127 | real | The “delta” value for the corresponding RMON counter during the interval. |
| Pkts128to255 | real | The “delta” value for the corresponding RMON counter during the interval. |
| Pkts256to511 | real | The “delta” value for the corresponding RMON counter during the interval. |
| Pkts512to1023 | real | The “delta” value for the corresponding RMON counter during the interval. |
| Pkts1024to1518 | real | The “delta” value for the corresponding RMON counter during the interval. |
| Filler2 | real | Reserved for future use. |
| Filler3 | real | Reserved for future use. |

## 10.3.6 Host Detail and Summary Tables

| Field | Type | Description |
|---|---|---|
| Agent | char(26) | Agent name. |
| Domain | char(15) | Domain name. |
| StartTime | int | Start time. |
| EndTime | int | End time. |
| StartTimeText | char(15) | Start time (text format). |
| EndTimeText | char(15) | End time (text format). |
| IfSpeed | int | Agent interface speed in bits per second. |
| NetType | char(4) | Agent network type: ET, TR, FDDI, or WAN. |
| Reinstalled | int | Reinstalled flag, non-zero if reinstalled. |
| Duration | int | Actual duration of interval in seconds. |
| Filler1 | int | Reserved for future use. |
| AddressType | char(4) | Host address type. |
| Address | char(20) | Host address, hex-ASCII format. |
| InUtilization | real | Average inbound utilization for time interval. |
| OutUtilization | real | Average outbound utilization for time interval. |
| InPkts | real | Packets in. |
| OutPkts | real | Packets out. |
| InOctets | real | Octets in. |
| OutOctets | real | Octets out. |
| OutErrors | real | Errors out. |
| OutBroadcastPkts | real | Broadcast packets out. |
| OutMulticastPkts | real | Multicast packets out. |
| Filler2 | real | Reserved for future use. |
| Filler3 | real | Reserved for future use. |

## 10.3.7 Conversation Detail and Summary Tables

| Field | Type | Description |
|---|---|---|
| Agent | char(26) | Agent name. |
| Domain | char(15) | Domain name. |
| StartTime | int | Start time. |
| EndTime | int | End time. |
| StartTimeText | char(15) | Start time (text format). |
| EndTimeText | char(15) | End time (text format). |
| IfSpeed | int | Agent interface speed in bits per second. |
| NetType | char(4) | Agent network type: ET, TR, FDDI, or WAN. |
| Reinstalled | int | Reinstalled flag, non-zero if reinstalled. |
| Duration | int | Actual duration of interval in seconds. |
| Filler1 | int | Reserved for future use. |
| AddressType | char(4) | Host address type. |
| SrcAddress | char(20) | Source host address, hex-ASCII format. |
| DstAddress | char(20) | Destination host address, hex-ASCII format. |
| Utilization | real | Average utilization for time interval, source host to destination host. |
| Pkts | real | Packets source host to destination host. |
| Octets | real | Octets source host to destination host. |
| Errors | real | Errors source host to destination host. |
| Filler2 | real | Reserved for future use. |
| Filler3 | real | Reserved for future use. |

# 10.4 Configuring Report Parameters

Even if you're planning to use ad hoc queries to generate your own custom reports, you still need to configure certain parameters. Aging parameters are those that control how long Trend Reporter saves information in various database tables. Poller parameters, on the other hand, are those that control what information, and associated time intervals, the Snapshot daemon is collecting.

## 10.4.1 Configuring Aging Parameters

To specify how long Trend Reporter waits before "aging out" (deleting) data from various tables, you need to configure aging parameters. You also use aging parameters to specify the minimum utilization percentage required before information is included in the database. To configure the aging parameters, turn to Configuring Aging Parameters on page 9-6.

## 10.4.2 Configuring Logging Parameters

To specify what agents, agent groups, or switches for wich you want to log information, you need to configure logging parameters for Poller. Poller is the function that lets you specify what specific data the Snapshot daemon collects. When you want to configure Poller logging for one or more agents, turn to Configuring Logging Parameters for Poller on page 9-7.

# CHAPTER 11 Decoding Captured Packets with Protocol Decode



One of *ForeView RMON* **ST**'s strengths is that its agents selectively gather network traffic in the form of frames from any operational segment node, or conversation. Agents store that information in an internal file and then transmit the file to *ForeView RMON **ST*** on command.

*ForeView RMON* **ST**'s Protocol Decode application reads the data file and breaks each captured packet into individual protocols. You can then view or print the raw data (in byte form).


The Data Capture application requires Roving or full RMON capabilities in the switch. The *ForeRunner* ES-3810 switch contains Roving RMON. The PowerHub 6000 and 7000 switches require a data sniffer or a network probe to gather network data before using Protocol Decode.


*ForeView RMON **ST*** can convert and use data captured in Sniffer format by Network General Corporation's Sniffer™ Network Analyzer.

The following sections contain more detailed information on Data Capture and Protocol Decode.

# 11.1 Understanding Protocol Decode

Protocol Decode lets you examine previously-captured data packets that are stored in a file that you define. You use the Protocol Decode function when you want to see the contents of individual data packets. You specify how you want the data decoded and displayed. You can also limit the amount and type of data displayed by specifying a filter to either pass or reject captured data frames that match its pattern.

You can use Protocol Decode on a file that contains previously captured or collected data, or as part of a real-time data capture process.

To use the real-time data capture process:

1. Start data capture at an agent, using Data Capture.
2. Stop data capture after an appropriate interval.
3. Upload the captured data to a file.
4. Examine the individual frames with full seven-layer decoding using the Protocol Decode application.

To decode previously captured or collected data:

1. Upload the previously captured data file to *ForeView RMON **ST***.
2. Perform post-capture filtering (optional).
3. Load the data into the Protocol Decode application.

Figure 11.1 shows the steps between Data Capture and Protocol Decode.

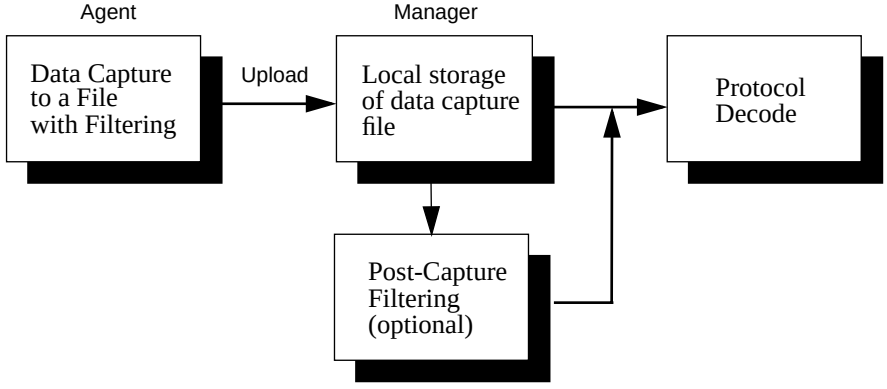



**Figure 11.1 -** Protocol Decode function

The following list shows the protocols that *ForeView RMON **ST*** protocol decode software supports.

| Ethernet | IEEE8023 | IEEE8025 | IEEE8022 |
|---|---|---|---|
| DODIP | DODARP | DODRARP | DODICMP |
| DODGGP | DODTCP | DODUDP | DODSMTP |
| DODFTP | DODTFTP | DODDNS | DODTLNT |
| DODNTB | DODNTDAT | DODNTNAM | DODSMB |
| NOVIPX | NOVSPX | NOVRIP | NOVECHO |
| NOVERRP | NCP | XNSIPX | XNSSPX |
| XNSRIP | XNSECHO | XNSERRP | XNSPEXP |
| XNSSMB | DECDRP | DECMOPDL | DECMOPRC |
| DECLAT | DECLDATA | DECNSP | DECSCP |
| DECDAP | DECNICE | DECFOUND | DECCTERM |
| DECSMB | APPLAP | APPARP | APPSDDP |
| APPLDDP | APPNBP | APPATP | APPZIP |
| APPRTMP | APPAEP | APPPAP | APPASP |
| APPDSP | APPAFP | VINESIP | VINESRTP |
| VINESARP | VINESICP | VINESIPC | VINESSPP |
| VINESMM | VINESST | VINEMAIL | SNMP |
| SUNNFS | SUNRPC | SUNMOUNT | SUNPMAP |
| SUNYP | SNAXID | SNATH | IBMNETB |
| SNARHREQ | SNARHRES | SNARU | SNAFM |
| SNAPS | IBMSMB | CLNS | ES-IS |
| TP 0/2/4 | ISO-Session | ISO-Presentation | FTAM |
| X400 | | | |

## 11.2 Capturing Data to a File Using Data Capture

Before you can use Protocol Decode, you must first capture packets selectively from an RMON agent and save them in a file. You can capture the traffic you want for either standard or user-defined protocols. Once you've captured the data you want to examine, you can analyze it using the Protocol Decode tool.


Data Capture requires Roving RMON capabilities in the switch. The *ForeRunner* ES-3810 switch contains Roving RMON. On the PowerHub 6000 and 7000 switches, network data must be captured using a data sniffer or network probe.

To decode packets captured with a data sniffer or in a previous Data Capture session, see Decoding Captured Data Using Protocol Decode on page 11-8. To set up a data capture session, use the following procedure.

1. If you haven't already done so, log in to the network management station where *ForeView RMON **ST*** is installed, and run the *ForeView RMON **ST*** application.
2. Select Delete to remove current data capture configuration in the agent. The capture setup is still configured until you delete it, even if the Data Capture window is closed.
3. Select an agent from the Agent list box in the *ForeView RMON **ST*** main window and click on the Data Capture icon or select Application/Data Capture from the menu bar. The Data Capture window is displayed as shown in Figure 11.2, with the agent name shown at the top of the window.

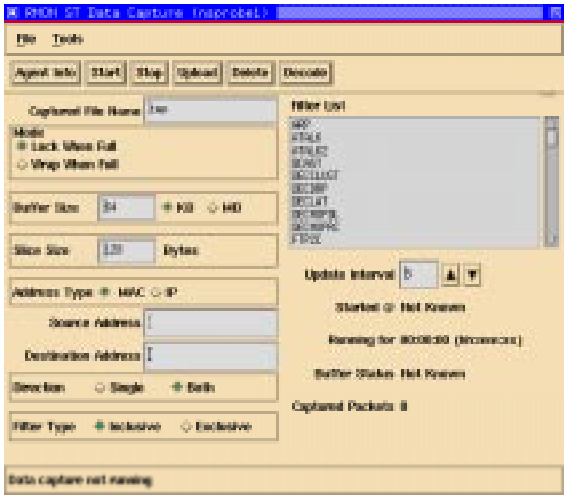



**Figure 11.2 -** Data Capture window

4. Enter the information in the appropriate fields in the Data Capture window. Each field is described in the following table.

| This field: | Lets you specify, or display: |
|---|---|
| Captured File Name | the name of the file where packets from the agent are uploaded. This file is stored in the usr/fore/foreview/fvr-mon/usr directory. The name is case-sensitive. The default file name is tmp.dat (*ForeView RMON **ST*** supplies the .dat extension for you). |
| Mode | whether the session stops when the capture buffer is full. **Lock When Full** stops the session when the capture buffer is full. **Wrap When Full** lets the capture session continue when the buffer is full, with the most recent packets overwriting the earliest, until you click on the **Stop** button. The default mode is **Lock When Full**. |
| Buffer Size | the maximum number of bytes to be saved in this capture buffer, including any implementation-specific overhead. Select either KB or MB. The range is from 32 - 8192 KB or 1 - 8 MB. The value must be a decimal number. The default buffer size is 64 KB. |

| This field: | Lets you specify, or display: |
|---|---|
| Slice Size | the maximum number of bytes of each packet that are saved in the capture buffer. For example, if a 1500-byte packet is received and **Slice Size** is set to 500, then only the first 500 bytes of the packet are stored in the associated capture buffer. The range is from 0 - 1518 bytes. If you set Slice Size to 0, the capture buffer saves the entire packet. The value must be a decimal number. The default slice size is 128 bytes. |
| Address Type | the address type as either MAC or IP. The address or symbol entered at Source and Destination Address is interpreted on this basis. The default address type is MAC. |
| Source / Destination Address (two fields) | the source and destination addresses. Valid MAC address, valid IP address, or valid Name are allowed. *ForeView RMON **ST*** uses these addresses to create more specific filters related to the source / destination of the data to be captured.<br>MAC addresses must be in this format:<br>01-23-45-67-89-ab<br>IP addresses must be dotted IP notation (for example: 204.205.206.207)<br>Name must be a valid host name. |
| Direction | whether to capture traffic from source-to-destination only (**Single**), or in both directions (**Both**), which is the default. |
| Filter Type | **inclusive** or **exclusive** capture properties. **Inclusive** (default) captures all traffic if the specified conditions *are* matched. **Exclusive** captures all traffic if the specified conditions are *not* matched. |
| Update Interval | the duration, in seconds, of the time between status field (described below) updates. The value must be a decimal integer.<br>The minimum (default) value is 5 seconds. The maximum value is 99 seconds. |
| Filter List | one or more filters from this list. Remember that the Filter Type field determines whether the filters you select are exclusive or inclusive. |

| This field: | Lets you specify, or display: |
|---|---|
| *ForeView RMON* ***ST*** updates the following status fields while you're running data capture: | |
| Started @ | the date and time when the packet capture function started. |
| Buffer Status | if capture is already on, Buffer Status displays "Running" and the time the capture was started. If capture is stopped, it displays "Stopped." If a capture entry does not exist, this field displays "Not Known". It also shows buffer status in brackets ("Full" or "Available"). |
| Captured Packets | the number of packets captured in the agent with the matched condition. This field is periodically updated during the capture sequence. |



5. Click on Start. This initiates an SNMP session that instructs the selected agent to begin collecting packets according to the filter definition.
6. Click on Stop to end the data capture session. The captured data is stored in a buffer in the agent. If you selected the mode **Lock When Full**, the data capture function stops automatically when the buffer becomes full.
7. Click on Upload to transfer the captured data from a buffer in the agent to the file you have specified in the **Captured File Name** field. The default file is tmp.dat.

When the upload process begins, a status report showing the number of packets uploaded is displayed in the lower margin of the window.

8. When you have uploaded the data and you want to decode it, use Protocol Decode from the *ForeView RMON* ***ST*** window, or click on the Decode button from the Data Capture window to initiate protocol decode.


You can decode the uploaded file at any time, by clicking on the Decode button from the Data Capture window, or Protocol Decode from the *ForeView RMON* ***ST*** main window.

## 11.2.1 Clearing the Data Capture Buffer

You may want to stop a data capture session and clear the buffer. To do so, click on the Delete button.

### 11.2.2 Getting Agent Information

To get a description of the agent you're using for data capture, use the following procedure.

1. Select Tools/Agent Info from the menu bar to display the Agent Information window (shown in Figure 11.3).


**Figure 11.3 -** Agent Information window

2. Click on **OK** to close the window.

To exit the Data Capture window, select File/Exit from the menu bar.

## 11.3 Decoding Captured Data Using Protocol Decode

Once you've captured data into a file, you can decode it, one frame at a time. In this section, you learn how to use Protocol Decode to examine captured data.

### 11.3.1 Loading a Data Capture File

Before you can perform a protocol decode, you must load the captured data file. To do so, use the following procedure.

1. Select File/Load from the menu bar in the Protocol Decode window. The Enter File Name window is displayed in Figure 11.4 on page 11-9.


**Figure 11.4 -** Enter File Name window

2. Select the directory and file that contains the captured data you want to decode from the list boxes. Use the directory filter to help you select files. To use the filter, enter a directory path and file filter, such as *.dat, then select Filter. Note that the data is stored in a file named xxx.dat.
3. Click on OK to load the data capture file.

**NOTE** The file information is displayed in the list box on the Protocol Decode window. The file information is listed by frame number.

## 11.3.2 Using Protocol Decode

Make sure the data you want to analyze is captured in a file, and you know the file name and path. Data Capture is described on page 11-4.

To see individual frames using Protocol Decode, use the following procedure.

1. Click on the Protocol Decode icon from the *ForeView RMON **ST*** Main window. The Protocol Decode window is displayed as shown in Figure 11.5 on page 11-10.

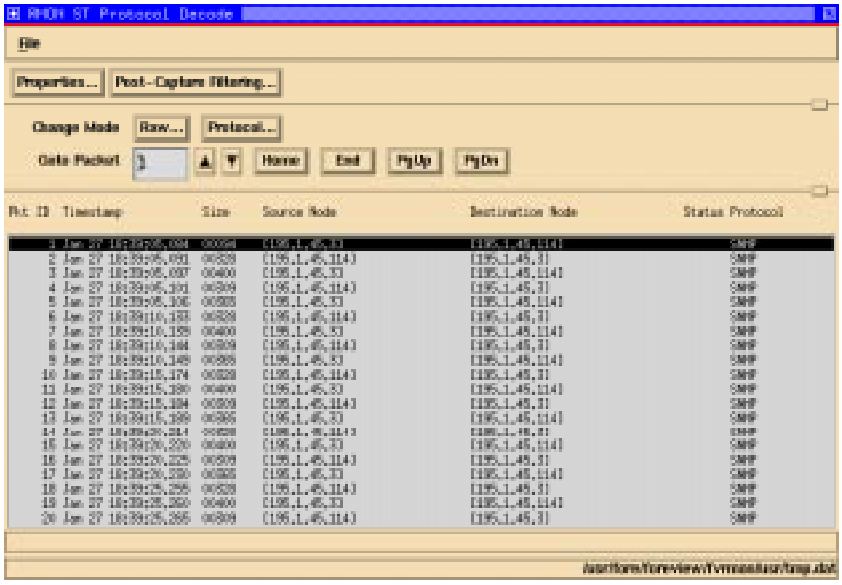



**Figure 11.5 -** Protocol Decode Window

2. Load the data capture file you want to examine. (See Section 11.3.1 below). The data is displayed in the **Protocol Decode** list box. Each line is one frame.
3. Select the frame you want to decode.
4. Using the Properties menu, determine how you want the data to be decoded. (See Selecting Protocol Decode Properties on page 11-10).
5. If needed, select Post-Capture Filtering for additional filtering. See Filtering Captured Data Using Post-Capture Filters on page 11-16.
6. Perform protocol decode in either Raw mode or Summary mode as described on Viewing Decoded Data in Raw Byte Form on page 11-13.

## 11.3.3 Selecting Protocol Decode Properties

Before you decode a frame, you can modify four properties that determine how decoded data in each mode is displayed. To determine protocol decode properties, select the Properties menu on the main Protocol Decode window. The Properties window is displayed in Figure 11.6 on page 11-11.


**Figure 11.6 -** Properties window



The selection fields simplify specifying the protocol decode properties. These fields contain toggle buttons that you can click to indicate your preferences. Make your selection for each field, then click on Apply to put your selections into effect, or Cancel to cancel the selections and return to the previous window. The following table describes each of the selection fields and its contents.

| This field: | Does this: |
|---|---|
| **Raw Mode** | determines whether the decoded bytes are displayed in Raw Mode as **ASCII** or **EBCDIC** characters. Default is **ASCII**. |
| **Time Mode** | determines whether the time displayed is the default value, **Absolute** (Month-Day-Time in *secs.msecs*), or **Delta** (difference between arrival of the current and previous frames, in *hh:min:sec:msecs*). |
| **Address Mode** | sets the Source / Destination address display as **Network** (IP), **Vendor**, or **Hex**. The default is **Network**. |
| **Zoom Mode** | enables and disables the multipaneled, multicolor effect in the seven-layer Protocol Decode window (page 11-15). Default is Enable. |

# 11.4 Performing Protocol Decode

There are four ways you can view a data capture file:

- **Summary Mode**. The complete file is displayed in the Protocol Decode window list box when you load it. Each line represents a frame of captured data. It has not yet been decoded.
- **Raw Mode**. A single frame you select is decoded and presented in raw byte form.
- **Protocol Decode** mode. A single frame you select is decoded and presented in full seven-level format.
- **Zoom Mode**. Any of the seven layers, as appropriate for the packet being decoded, can be displayed in the full window.

You'll learn more about each of these modes in this section.

## 11.4.1 Viewing a Data Capture File in Summary Mode

Before you perform a protocol decode, the file you selected is displayed in summary mode in the list box on the Protocol Decode window. Each frame is represented by a single line numbered from 1 to N, where N is the total count of frames in the capture buffer, as shown in Figure 11.2 on page 11-5.

The summary mode list box contains a number of headings with values shown below. The summary mode list box information includes:

- **Pkt ID.** The index number of the frame, starting with 1. You can scroll through the list of frames by using the cursor. The frame currently selected is highlighted.
- **Timestamp.** The timestamp indicating the date and time this frame was captured. The format of the timestamp is: *Month Day hh:mm:ss:ttt*. For example:

  `Dec 7  17:32:25.569`.
- **Size.** The number of bytes in the frame.
- **Source Node.** The address of the node that sent that frame. If Vendor Name is the default, however, the name of the node is displayed instead.
- **Destination Node.** The address of the destination node specified in the frame. If Vendor Name is the default, however, the name of the vendor is displayed instead.
- **Status.** If a frame is faulty, the type of fault (more than one may apply):
  - **R** indicates a runt frame (a frame less than 12 bytes long).
  - **J** indicates a jabber frame (a frame more than 1518 bytes long).
  - **C** indicates a CRC / alignment error frame.

- **P** indicates a processing error. For example, Frame #40 with a processing error indicates that the agent was not able to process packets just prior to capturing Frame #40.

- **Protocol.** Identifies the highest-level protocol in that frame.

The selection buttons in the Protocol Decode window (Summary Mode) let you specify the parameters for the decoding function. The selections buttons include:

- **Change Mode.** Lets you switch directly to Protocol Mode or Raw Mode.
- **GoTo Packet.** Use **GoTo Packet** to show the first frame on the first line (**Home**) or the last frame on the last line (**End**). Selecting either selection initiates the action. You can use the scroll arrows to scroll either forward or backward through the frames.
- **Packet Number.** Inserting a frame number in the **Packet Number** field causes that frame to appear on the first line.



## 11.4.2 Viewing Decoded Data in Raw Byte Form

Raw mode presents decoded data in raw byte form. To view protocol information in Raw Mode, Select Raw in the **Change Mode** field on the main Protocol Decode window. The Raw Decode window is displayed as shown in Figure 11.7. Note that the name and path of the capture file is displayed at the bottom of the window. The list box headings include **Frame Number**, **Size**, **Arrival Time**, and display mode (**ASCII** or **EBCDIC**).

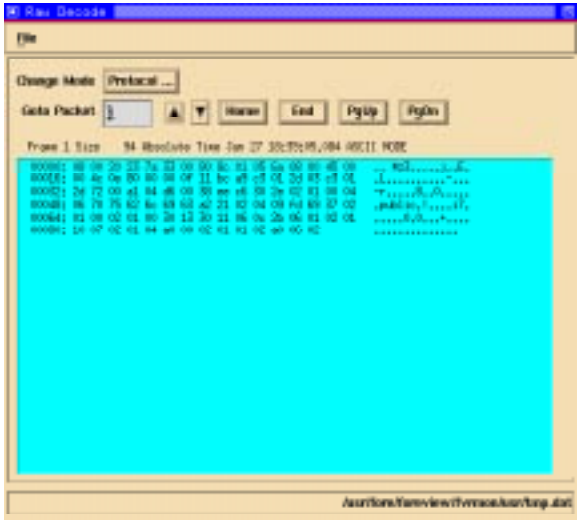



**Figure 11.7 -** Raw Decode window

The selection buttons in the Raw Decode window let you specify the parameters for the decoding function. The selections are described in the following table.

| This selection button: | Lets you: |
|---|---|
| Change Mode | switch directly to Protocol Mode. |
| GoTo Packet | jump immediately to either the first frame displayed in the list box (**Home**), or the last (**End**). |
| Packet Number | display a specific frame in the list box. Inserting a packet number in the **Frame Number** field displays the raw decode of that frame. Selecting the up/down arrows in the **Frame Number** field causes the raw mode frame display to scroll up or down one frame at a time. |

## 11.4.3 Viewing a Frame in Seven-Level, Decoded Format

Selecting Protocol in the **Change Mode** field of either the Protocol Decode window or the Raw Decode window displays the highlighted frame in seven-level, decoded format. The decoding is fully automatic and causes the frame to display in up to seven list boxes, corresponding to successive layers of the protocol.


**Figure 11.8 -** Protocol Decode window, seven-level decode display

Use the scroll bars on the list boxes to scroll through each protocol layer and examine the contents of each layer (of the ISO seven-layer model) shown in readable format. If the frame contains no identifiable protocol after a certain layer, the rest of the frame is displayed as a raw dump in the last list box, labelled User Data.

## 11.4.4 Viewing a Single Protocol Layer Using Zoom Mode

Select Zoom using the Change Mode selection button in the Protocol Decode window to see a full display of any protocol layer contained in the current frame as displayed in the Zoom Decode window. The Zoom Decode window lets you scroll back and forth through protocol layers by clicking the Next Layer or Prev Layer selection buttons. The display wraps from the highest layer back to the lowest layer decode, and vice versa. Figure 11.9 on page 11-16 shows the Zoom Decode window.

You can see new frames by using any of the techniques described earlier, to scroll through the frames displayed in the Summary Mode window.

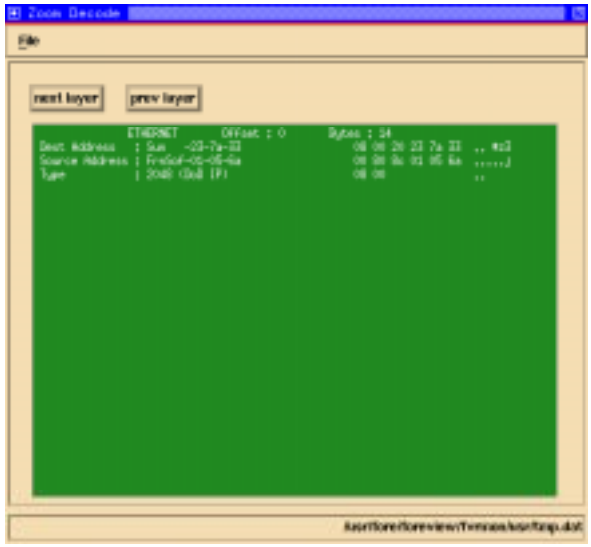



**Figure 11.9 -** Zoom Decode window

## 11.5 Filtering Captured Data Using Post-Capture Filters

Sometimes you may want to filter previously captured data to isolate protocol information you need. You can do this using the Post-Capture Filters. The following procedure steps you through the process.

1. Load the data capture file; to do so, see page 11-8.
2. Select Post-Capture Filtering from the Protocol Decode window. The Post-Capture Filters window is displayed as shown in Figure 11.10 on page 11-17.

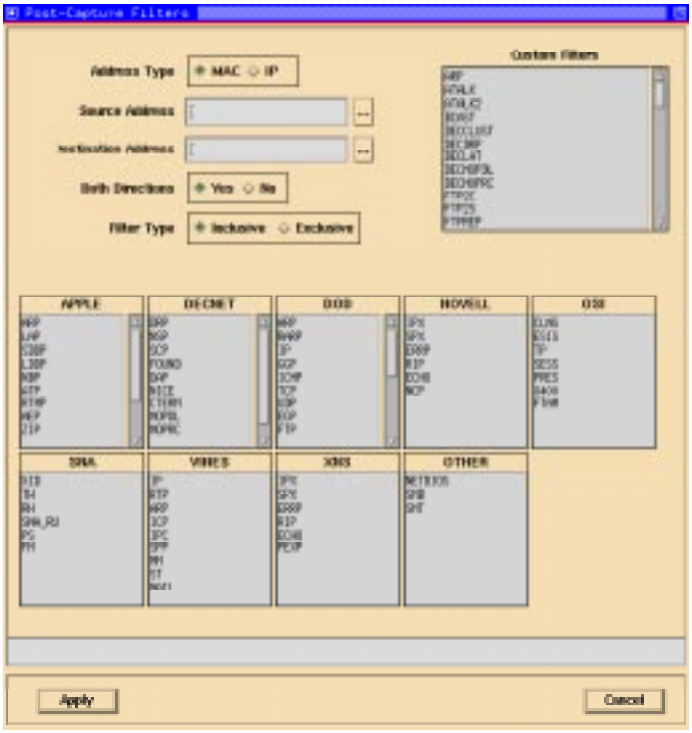



**Figure 11.10 -** Post-Capture Filters window

3. Select the filter definition you want to use.
4. Select Apply. The **Summary Mode** list box on the Protocol Decode window now contains only packets that have passed your Post-Capture Filter definition.
5. The selection fields simplify specification of the parameters for post-capture filtering. These fields contain toggle buttons that you can click to indicate your preferences. The selections include:
   - **Address Type.** You can specify the address type as either MAC or IP. The address or symbol entered in the Source and Destination Address field are interpreted according to this setting. You can select any valid MAC address, IP address, or name. Use these addresses to create more specific filters related to the source or destination of the data to be captured.
   - **Source/Destination Address.** Select Source Address or Destination Address to specify source and destination addresses for filtering.

- **Both Directions.** Determines whether to capture traffic from source-to-destination only, or in both directions. Select Yes to filter data in both directions, No to filter data in only one direction.
- **Filter Type.** Can be either inclusive or exclusive. Inclusive means capture all traffic if the specified condition is matched. Exclusive means capture all traffic that does not meet the specified condition.

# PART 2

# Using *ForeView RMON **ST*** With External Network Probes

This part describes *ForeView RMON **ST*** applications that require network probes. Network probes are optional hardware devices with embedded RMON agents. The *ForeView RMON **ST*** software will work with many of the agents embedded in network probes to enhance Network Monitoring capabilities. If you are using a NETscout Probe from Frontier Software, see APPENDIX D for additional information.

This part contains the following chapters:

# CHAPTER 12 *ForeView RMON ST* and Network Probes



*ForeView RMON **ST*** supports RMON2, RMON, Proxy RMON, roving RMON, mini-RMON, and proprietary MIBs. *ForeView RMON **ST*** uses them to continuously monitor all switch ports when needed. However, RMON and RMON2 functions in *ForeView RMON **ST*** are dependent on the network probe or switch capabilities. Mini-RMON is embedded in the PowerHub 6000 and PowerHub 7000 LAN Switches and roving RMON is embedded in the *ForeRunner* ES-3810.

If you wish to take advantage of the extra functionality of full RMON MIBs, you will need a network Probe. Proprietary MIBs and Proxy RMON used by *ForeView RMON **ST*** require a NETscout Probe from Frontier Software.

With a network probe, you can provide complete monitoring and analysis of all ports on a selected switch. In addition, *ForeView RMON **ST*** lets you monitor critical interswitch links using dedicated high-speed probes. *ForeView RMON **ST*** can aggregate the data from mini-RMON, roving RMON, and any dedicated probes you've defined into a consolidated monitoring and diagnostic environment supporting switch and VLAN (Virtual LAN) traffic.

For more detailed information on how network probes utilize the different implementation of RMON, see the following sections:

## 12.1 Mini-RMON

Mini-RMON is a subset of standard RMON. It is supported directly on the PowerHub 6000 and PowerHub 7000. Because standard RMON is supported by network probes, mini-RMON is not discussed here; it is discussed in Section 3.7.2 on page 3-11.

## 12.2 Roving RMON

Roving (or Roving RMON) refers to how *ForeView RMON **ST*** can direct full RMON analysis to any switch port you select, as long as the agent and the switch support the RMON standard. *ForeView RMON **ST*** implements Roving automatically, whenever you launch an application or tool that requires any of the five remaining RMON groups beyond mini-RMON: Hosts, Hosts Top N, Conversations, Filters and Data Capture. A switch supports Roving when it meets the following two requirements.

- There is an analyzer port, or a port that's not transmitting network traffic that you can designate as an analyzer port.
  *and*
- The switch supports mirroring—the ability to direct a copy of traffic from a monitor port to the analyzer port where the roving probe can view that traffic.

Roving involves adding a roving agent to the desired port on the *ForeRunner* ES-3810 switch or, if you have a PowerHub system, attaching a roving agent to the desired port, connecting a network probe to an analyzer port on the switch, then "mirroring" traffic from a selected switch port to that analyzer port. In its most basic sense, a copy of the monitor port traffic is directed to the analyzer port where the probe or agent is attached. The switch or probe then examines this traffic as if it were receiving the traffic directly. Although the analysis port is a static, physical connection on the switch or to the probe, *ForeView RMON **ST*** dynamically sets the monitor port to the switch port you choose to analyze.

Once *ForeView RMON **ST*** detects a problem on a port, additional data is often needed to resolve it, including extensive data captures, and network layer host and conversation lists. You can then use Roving to bring the full RMON power of the agents on the switch, or the RMON / RMON2 power of a NETscout Probe, to the suspect port for detailed monitoring and analysis.

For example, if you notice an unusually high amount of network traffic on a specific port. You can run Domain Manager in Switch mode and then choose to launch Conversation List, TopN Talkers graph, or All Talkers list for the port's RMON domain to identify the reasons for all that traffic. At that point, *ForeView RMON **ST*** automatically roves to the specified port to analyze that traffic and retrieve the host and conversation statistics needed.

## 12.3 Dedicated Probes and Critical Links

Interswitch links are the backbones of switched LANs. Equally important are high speed media connections to servers. Because these critical links handle high volumes of traffic, they are usually FDDI or Fast Ethernet type media. Continuous monitoring of these links is important for managing growth and immediately troubleshooting problems. To do so, you can attach Fast Ethernet and FDDI probes directly to these critical links to provide continuous full RMON/RMON2 monitoring and analysis. You can then include these dedicated probes as part of the switch definition when you add a switch to *ForeView RMON* ST, and even tailor your agent group to display all dedicated trunk probes, server probes, or both.



## 12.4 Proxy RMON

Proxy RMON lets you monitor switches that do not have embedded RMON as if they had embedded mini-RMON on each switch port. Proxy RMON uses an external NETscout Probe to map a switch's private MIBs to one mini-RMON group: statistics. *ForeView RMON **ST*** then polls the probe (also referred to as the proxy agent) for this mini-RMON information. In this way, you can monitor switch port traffic in terms of mini-RMON values. Because the FORE Systems' LAN switches have Roving RMON or mini-RMON embedded in them, Proxy RMON is usually unnecessary.

### 12.4.1 Proxy RMON and Embedded RMON Devices

As mentioned earlier, the most common reason to use a proxy RMON agent is to provide RMON support on behalf of a device that does not have embedded RMON. But there are times when you may want to use proxy RMON to monitor a device that does have embedded RMON support.

In such a case, the RMON counters within the device map directly to the corresponding mini-RMON groups within the proxy agent. Some of the reasons you may want to set up a proxy agent to monitor an embedded RMON device include:

- **One point monitoring.** If you have multiple *ForeView RMON **ST*** applications polling the device for RMON-related information, you may want to set up a single proxy agent to poll the device, and have the multiple *ForeView RMON **ST*** applications poll the proxy agent instead. This reduces CPU requirements in the device. For example, if you launch Traffic Monitor, Segment Zoom, Segment Statistics, and Short and Long-Term History graphs to monitor a switch, each of these applications will poll the switch for RMON data. Instead, set up a NETscout Probe to proxy the switch, and let the multiple *ForeView RMON **ST*** applications poll the agent.

- **The probe is more accessible than the switch.** For example, a management station may be monitoring a network segment connected through an out-of-band SLIP connection to the probe, but does not have direct access to a switch. The probe can be used to proxy the switch and provide RMON information on behalf of each switch port.
- **Limited resources.** An embedded RMON device may not have the resources needed to implement certain RMON groups. In this case, you can enable only the statistics group on each port, and set up an external proxy agent to monitor the device. The proxy agent will perform SNMP GETs to retrieve those statistics and map them to the remaining mini-RMON groups. That same proxy agent could also be used to focus full RMON on a selected port if the device supports roving RMON and the probe has the needed analyzer port connection.

## 12.5 About RMON2

RMON2 support is necessary when you need to monitor and troubleshoot at layers higher than data link. With *ForeView RMON **ST***'s RMON2 support, you can monitor traffic at network and application layers. RMON2 support, you can get statistics for all hosts accessing a specific segment, no matter where the hosts are located, or how the network is connected.


RMON and RMON2 function in *ForeView RMON **ST*** are dependent on the network probe or switch capabilities. The network probe or switch deployed in the network must contain or support RMON and RMON2 agents before *ForeView RMON **ST*** can monitor and troubleshoot networks at layers higher than data link. Currently, the FORE Systems' LAN switches do not contain RMON2 agents.

With RMON2, RMON groups map into all of the major network layer protocols, such as IP, IPX, DECnet, Appletalk, Vines, and OSI. Also, as mentioned earlier, you can monitor application layer traffic, so you can monitor network applications such as Notes, Telnet, Microsoft Mail, and Sybase, among others. You can do so because RMON2 outlines how you can construct logical filters for remote agents. This means that *ForeView RMON **ST*** can now monitor and help you troubleshoot key application-layer traffic within the enterprise network.

# 12.6 Configuring a NETscout Probe

The following example shows how to configure a NETscout Probe from Frontier Software to function as a Roving RMON agent and monitor a PowerHub 7000 switch. As a Roving RMON agent, all ten RMON groups can be monitored on a per-port basis. If you have a different type of network probe, or if you want to take advantage of some of the more advanced features of your network probe, see the documentation that came with your probe for configuration information.

If you have a *ForeRunner* ES-3810 switch, consult the documentation that came with the switch and the probe for information on configuring the agents in the probe to function with your switch.



Before you configure the NETscout probe to monitor your network, you need to make sure that the following conditions exist:

- You have a two-port NETscout Ethernet Probe. (One port is for receiving and snooping the mirrored packets and the other for reporting to the management console running *ForeView RMON **ST***.)
- The NETscout Ethernet Probe has been configured and you know its IP address. (See Remote Login on page D-26 or the *NETscout Probe User Guide* for more information on configuring your NETscout Probe.)
- The Probe is attached to the correct ports using the correct cables. (See the *NETscout Probe User's Guide* for more information.)
- You have added the switch in the *ForeView RMON **ST*** **`Switches`** selection box.
- Port monitoring is disabled for all ports on the PowerHub switch. To see the current port monitoring state, log into the PowerHub 7000 and issue the following command from the management subsytem of the PowerHub switch:

  **port-monitor**

  See the Port Monitoring section of the PowerHub's hardware manual for information on disabling Port Monitoring if the port monitor command shows any segments being monitored.
- Packet forwarding is disabled on the PowerHub switch port attached to the snooping port on the NETscout Ethernet Probe.

To configure the NETscout Probe to function as a Roving Agent:

1. Using a text editor, edit the `default.dvp` file to reference the switch and port that the NETscout probe is connected to. The `default.dvp` file is found in the `/usr/fore/foreview/fvrmon/usr` directory. The `default.dvp` is shown in Figure 12.1 on page 12-6.

- Add the following line at the bottom of the default.dvp file:

  **<Switch_Name>:<Port>**

  where:
  **<Switch_Name>** is the name you have given the switch in the Add Switch dialog box.
  **<Port>** is the port number of the port attached to the Probe. In the following example, the switch is named PH7000 and port 6 on the PowerHub is connected to the snooping port (port 3) on the NETscout Probe.

2. Save the changes to the default.dvp file and restart *ForeView RMON **ST***.

```
#
# Domain View Properties (File: default.dvp)
#
probe-read-community:     "public" # default read community for probe
probe-write-community:    "public" # default write community for probe
switch-read-community:    "public" # default read community for switch
switch-write-community:   "public" # default write community for switch
short-history-buckets:    50# number of buckets
short-history-interval:   30# interval in seconds
long-history-buckets:     50# number of buckets
long-history-interval:    600# interval in seconds
nl-convs:                 2000# number of Network Conversation
al-convs:                 10000# number of Application Conversation
net-to-mac-hosts:         1000# number of Network to MAC address
enable-fast-upload:       yes     # yes/no
enable-dte-dce:           yes     # yes/no
default-printer:          "lp" # default printer
lines-per-page:           66 #lines per page while printing/storing
                             # to a file
enable-start-end-util-calc:  0# 0=old method, 1=CalcUtil end-start
Ph7000:                   6# Roving port on PowerHub
```

**Figure 12.1 -** The default.dvp file.

3. Make sure that port 3 on the probe is connected to the monitoring port on the PowerHub switch, and that the the other port on the probe is connected to any other port on the PowerHub switch that has forwarding enabled.
4. Add the NETscout Probe as an agent to the **Agents [All]** group in the *ForeView RMON **ST*** main window. (See Adding a New Agent on page 4-3 for information on adding agents.)
5. Set the interface to "3" in the **`Interface Number`** field of the **`New Agent`** window. Make sure you put the IP address of the probe in the **`IP address`** field and not the IP address of the PowerHub switch.
6. Edit the PowerHub switch's profile by highlighting the switch's name in the **`Switches`** selection box and choosing **`Edit`** from the buttons on the right of the Switches selection box. Add the name of the NETscout Probe in the **`Roving Agent field`**.

Roving RMON is now enabled on the hub.




If you are using a network probe from a vendor other than Frontier Software, you must configure port monitoring using *ForeView* 4.x or the PowerHub switch's command line interface. See the appropriate PowerHub switch's Installation and Configuration Manual or the *ForeView Network Management 4.x User's Manual* for more information about configuring Port Monitoring.

# CHAPTER 13 *ForeView RMON ST* Domains and Network Probes



This chapter covers RMON Domains as used by *ForeView RMON **ST*** in different RMON applications. This chapter also includes other information that applies specifically to network probes and how the probes can be utilized in the network by ForeView *RMON **ST***. If you have a NETscout Probe, see Appendix F for additional applications that take advantage of Frontier Software's Proprietary MIBs.

When you're working with *ForeView RMON **ST,*** the term "domain" is used to describe the kinds of traffic for which you want to see statistics. A domain lets you choose to display a specific traffic stream. For example, when you choose to view statistics for the IP domain, you'll see information about *just* the IP traffic on a network segment you select.

For more detailed information on domains and how they relate to network probes and *ForeView RMON **ST***, see the following sections:

# 13.1 *ForeView RMON ST* Domains

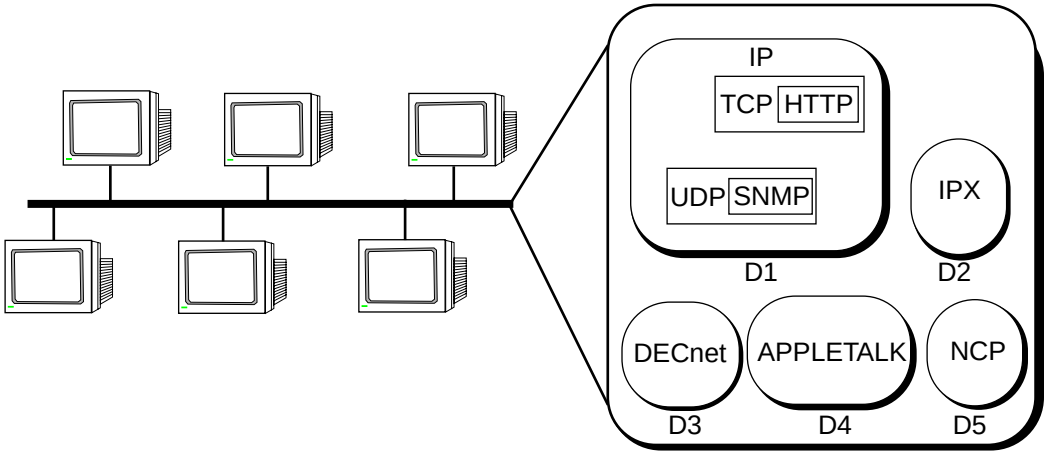
Domains are flexible, and can reflect different kinds of traffic. In fact, domains can display traffic for any of the following layers (shown in the OSI model):

- **MAC layer**. This includes basic RMON protocols that operate on the data link and physical layers. For example, *ForeView RMON* ***ST***'s RMON domain is a MAC-layer protocol. FORE Systems' LAN Switches can access, interpret and display information gathered from this layer.
- **Network layer**. This includes protocols that operate on the Network layer. For example, IP and IPX are Network-layer protocols. At this level, you can monitor network traffic by host and conversations for various network protocols and for such standard RMON information as utilization, packet rate, errors, etc. FORE Systems' LAN Switches can access, interpret and display RMON information gathered from this layer. The Host and Conversation groups are not available on the PowerHub Switches without the use of a network probe. The *ForeRunner* ES-3810 can gather Host and Conversation information on a per-port basis.
- **Application layer**. This includes protocols that operate from the Transport layer to the Application layer. For example, SNMP and TFTP are Application-layer protocols. This layer is functional on the FORE Systems' LAN Switches only with the use of network probes.

In the *ForeView RMON* ***ST*** architecture, a domain is a definable variable that can include one protocol or a group of protocols (Figure 13.1). You would use a domain to see all traffic on a network segment that matches the protocol specified in the domain. Many commonly-used protocols (for example, IP, IPX) are predefined *ForeView RMON* ***ST*** domains. The predefined RMON domain includes all supported protocols, allowing you to see all traffic on a network segment.

*ForeView RMON* ***ST*** lets you define your own domains. This is useful to let you monitor very specific traffic patterns that reflect your organization's needs. For example, to get an idea of the IP and IPX traffic on a network segment, define a domain to include only IP and IPX. Then apply that domain on the network segment. The results show you how much of the segment's utilization is strictly IP and IPX traffic.

In order to fully utilize the domain features of the software, you must be able to apply filters to isolate the different protocols. Filters are not available in the mini-RMON Groups, but can be done with a network probe that supports RMON2. Figure 13.1 on page 13-3 shows how filters can be used to isolate different protocols.




**Protocol & Domain Relationship On Network**

**D1=**IP protocols and "child" protocols TCP (with its child HTTP) and UDP with its child SNMP). You can create one domain to include these IP-related protocols or create a separate domain for each protocol

**D2=**IPX protocol

**D3=**DECnet protocol

**D4=**AppleTalk protocol

**D5=**NCP protocol

You could choose to group specific protocols together to form one domain. For example, if you group IPX (**D2**) and NCP (**D5**) into a domain you name LAB, when you apply domain LAB, only traffic using the IPX and NCP protocols is displayed. When you want to see all traffic, use the domain RMON (includes all supported protocols).

**Figure 13.1 -** Domain example

Notice in Figure 13.1 - that you can use predefined domains to get RMON statistics for specific protocols, or add a custom domain, such as LAB, to get RMON statistics for that domain. The special predefined domain, RMON, provides RMON statistics for all the traffic on the segment.

## 13.2 The OSI Protocol Model

Protocols are the rules that data communications devices use to carry out their communication processes. The generalized model for protocols is the Open Systems Interconnections (OSI) model (Figure 13.2). This model includes seven layers, each of which carries out a specific subset of the communications process. The model is often described as a stack or suite. By looking at a protocol stack, you can often identify network malfunctions.

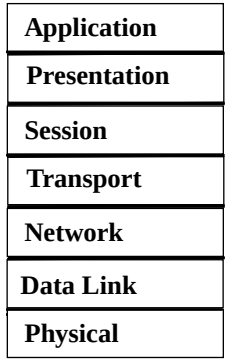



**Figure 13.2 -** OSI model

Each layer within the OSI model performs specific functions. Starting at Data Link, any given layer depends upon the layers beneath for "support" so it can perform its functions correctly. For example, protocols at the Network layer can smoothly deliver packets to the correct addresses only when the Data Link and Physical Link layers are configured and are operating correctly. Each layer contributes to network communications as follows:

- **Physical layer**. Specifies physical and electrical characteristics of connections that make up the network, such as twisted-pair cables, coaxial cables, repeaters, and so on. Sometimes called hardware layer.
- **Data-Link layer**. Recognizes electrical representation of the data (bit patterns, encoding methods, and so on). Errors are detected at this level and corrected by requesting retransmission of corrupted packets.
- **Network layer**. Switches and routes packets to get them to correct destination; addresses and delivers message packets.
- **Transport layer**. Controls message component sequencing and regulates inbound traffic flow with more than one packet in process. Recognizes and discards duplicate packets.

- **Session layer**. Lets applications running at two workstations coordinate their communications into a single session. Supports session creation, manages packets sent back and forth during the session, and terminates the session.
- **Presentation layer**. Converts data either into or from a particular machine's native internal numeric format.
- **Application layer**. Point where a message to be sent across the network enters OSI model. User interfaces are here at this layer.

## 13.2.1 The *ForeView RMON ST* Protocol Model



Various network protocols (such as IBM, TCP/IP, DECnet, Vines, among others) are based on the OSI model. As an example, a protocol-interpreter suite is shown below. Notice the correspondence with the standard OSI model.

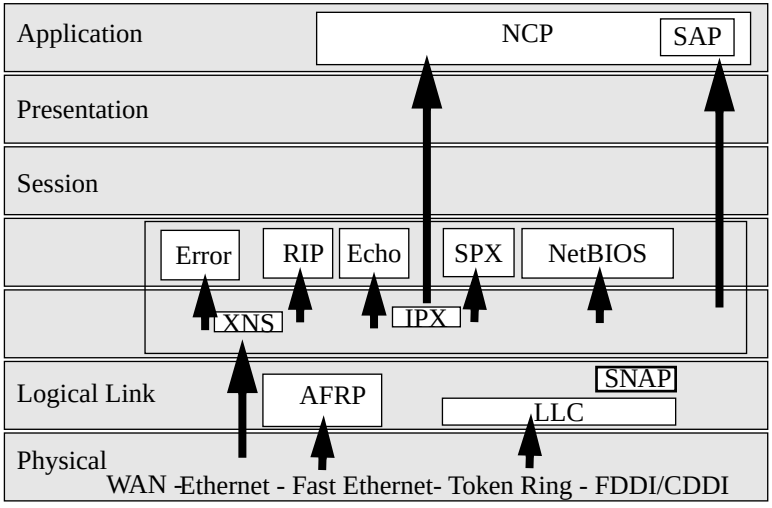



**Figure 13.3 -** Example *ForeView RMON **ST*** protocol interpreter suite

*ForeView RMON **ST*** contains a set of filters used to isolate an individual protocol from other network traffic. A second filtering process (domains) separates the components of the protocol stack for each supported protocol. Now, using Data Capture, you can select only specific traffic in a segment, such as IBM traffic, by using a filter that passes only IBM traffic. Then you use Protocol Decode to separate each packet (also called a "frame") into its component layers and

decode each layer according to the selected protocol.

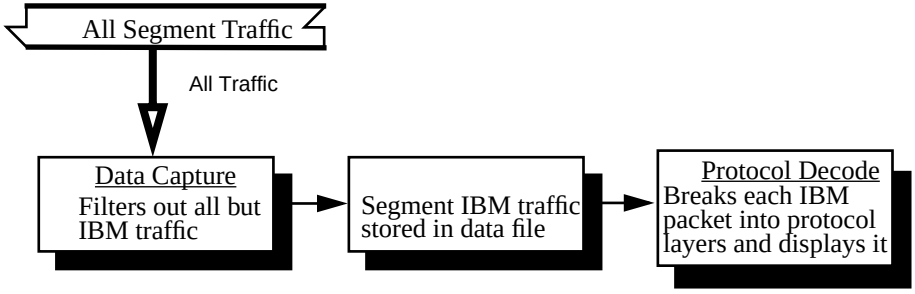



**Figure 13.4 -** Extracting and decoding IBM traffic from a network segment

# 13.3 Using Domains

The original RMON standard supports network monitoring of link-layer traffic only. This limits RMON to presenting statistics only for aggregate traffic, not statistics for the different layers of various protocol stacks (such as IP, FTP, IPX). Because it is not capable of monitoring at the network layer, an RMON device cannot distinguish traffic on its segment that originated across a router. By not monitoring above the MAC layer, many useful applications, such as monitoring WAN links, measuring client-server response time, or providing seven-layer protocol statistics, are not possible.

Domains provide an architecture that allows the monitoring of network traffic for all seven ISO layers within the framework of the RMON standard. Using domains lets you monitor any protocol traffic for any device or subnet on any segment of an enterprise network.



## 13.3.1 About Domains in *ForeView RMON* ST

In *ForeView RMON* ***ST,*** you can choose to add two types of domains: protocol or generic. Protocol domains are those that work only with RMON2. You can add, edit, or delete protocol domains for protocols in the data-link, network, and application layers. Protocols for each of these layers are supplied with *ForeView RMON* ***ST*** in special *.inf files. This means that whenever you want to add or edit protocol domains, the *.inf files contain all of the protocol definitions that you'll need. We recommend that you do not edit these *.inf files, because a network probe wouldn't recognize any protocol definition other than those that are shipped with the product.

Generic domains are those that support Frontier Software's enterprise MIBs. For generic domains, *ForeView RMON* ***ST*** supports the MAC, NET, and SUBNET address modes. In the MAC address mode, host and matrix tables are built using the six-byte physical-layer MAC address as specified by the RMON standard.


Enterprise MIBs are proprietary MIBs from Frontier Software, and can only be utilized if you are using a NETscout Probe network probe.

*ForeView RMON* ***ST*** includes the RMON domain, which is used with third-party RMON agents to monitor MAC-level (basic) RMON statistics. In the NET address mode, *ForeView RMON* ***ST*** creates host and matrix tables containing network addresses for IP, IPX, and DECNET packets.

- For IP packets, the NET-mode address is the four-byte IP address (example: 45.20.0.20).
- For IPX packets, the address is the IPX host address (example: 08002B534256).

- For DECNET packets, the address is the area.node address (example: 1.1023).

SUBNET address mode is similar to NET address mode, except that the agent uses subnet addresses for collection purposes. As a result, the host and matrix tables contain total statistics for each subnet. *ForeView RMON **ST*** uses only IP, IPX, and DECNET packets to create the tables.

Managing remote network segments is critical to providing high network availability. Key network management standards such as RMON and SNMP are the technology enablers to build the tools, such as *ForeView RMON **ST,*** to manage distributed networks.

- With RMON, you can gather network statistics for problem resolution. Active monitoring alerts you to problems before they become critical.
- With domains, you can monitor many more network traffic parameters, devices and LAN segments for the most effective and focused problem resolution.
- With SNMP, you can poll device status from a central site.

# CHAPTER 14 Monitoring Token Ring Networks



*ForeView RMON **ST*** has the ability to manage statistics gathered from the Ring Station RMON group. However, the RMON agent that is used must also support the Ring Station group. The Ring Station group is an RMON extension that is included by *ForeView RMON **ST*** in the Basic RMON MIB. Ring Monitor can be used to configure, display, and print Token Ring statistics collected using a network probe that supports the Ring Station MIB group, which is group 10 of the RMON MIB.

**NOTE**

Not all network probes support group 10 of the RMON MIB. Check your network probe documentation to make sure the option is supported before attempting to configure Ring Monitor.

The RMON MIB is defined in RFC 1757. The Group 10 Token-Ring specific extensions are defined in RFC 1513. Group 10 is enabled automatically whenever a Token Ring agent is powered on and finishes its initialization sequence.

For more information on Ring Monitor, see the following sections:

# 14.1 Viewing the Ring Station List for a Token Ring Agent

Use the following procedure to launch Ring Monitor from the *ForeView RMON **ST*** main window and display Ring Monitor's Ring Station List for the agent you select.

1. If you haven't already done so, log in to the network management station where *ForeView RMON **ST*** is installed, and run the *ForeView RMON **ST*** application.
2. Select a Token Ring agent from those shown in the **Agents [All]** list box or select the agent group containing the Token Ring agent you want to monitor. (If the agent you want is not listed, see Chapter 4 in this manual for information on adding an Agent.)
3. Click on the Ring Monitor icon in the *ForeView RMON **ST*** window, or select Application/Ring Monitor from the menu bar.

The Ring Station List window, showing the default Status View, is displayed. Figure 14.1 shows the Ring Station list. The status view shows a list of the stations the agent has seen since it was powered on. You can sort this listing in a number of ways. Status View is the default view. You can also select a Summary View, shown in Figure 14.2 on page 14-3.

**Figure 14.1 -** Ring Station List (status view)

## 14.1.1 Selecting Views

You have a choice of two Ring Monitor views: **Status View** and **Summary View**. Each view provides different information in the window's list box.

- **Status View** is the default view. It provides a list of the stations the agent has seen since it was powered on, and provides basic information about each station.
- **Summary View** provides an error summary for each station.

To select a view, use the following procedure:

1. Select the View menu.
2. Click on either Status or Summary. One of the following is displayed:
   - **If you selected** View/Status, the Ring Station List (status view) is displayed (Figure 14.1 on page 14-2).
     *or*
   - **If you selected** View/Summary, the Ring Station List (summary view) is displayed (Figure 14.2).



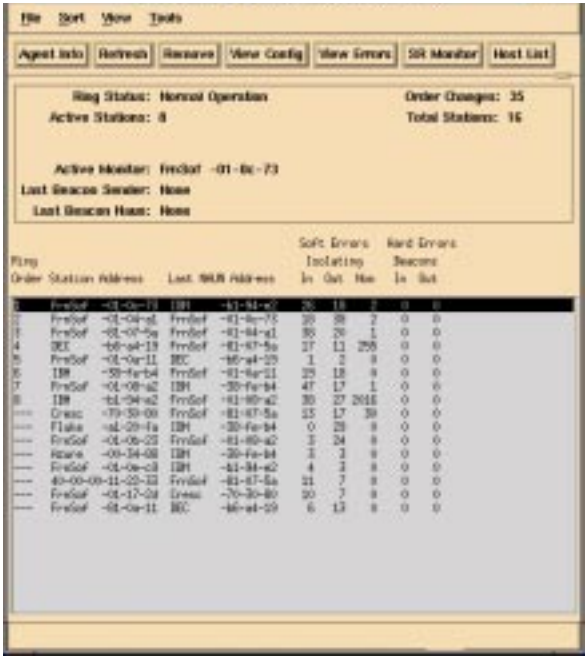



**Figure 14.2 -** Ring Station List (summary view)

## 14.1.2 Understanding the Ring Station List

The Ring Station List box contains several headings with values shown below. The Ring Station List shows different information about the stations on the ring depending on the view you selected. The tables below give you an idea of the information being displayed. The list box contains the following information when you choose the status view:

| This Status View list box heading: | Shows you: |
|---|---|
| Ring Order | the order of this station in the ring. |
| Station | the name of the station. |
| Address | the address of the station. |
| Last Enter Time | the last time the station entered the ring. |
| Last Exit Time | the last time the station exited the ring. |
| RIns | ring insertions. The number of times a station has been inserted into the ring. |
| Dups | duplicate addresses. |
| Status | whether a station is active or inactive. |

When the Ring Monitor window is in Summary View, the list box contents are as described below.

| This Summary View list box heading: | Shows you: |
|---|---|
| Ring Order | the order of this station in the ring. |
| Station Address | the address of the station. |
| Last NAUN Address | the address of the nearest active upstream neighbor (NAUN) of the station (specified in the Station Address field). |

| This Summary View list box heading: | Shows you: |
|---|---|
| Soft Errors | soft errors that occur normally in the ring. Soft errors do not cause the network to come down, and are one of two types: isolating and non-isolating. An isolating soft error is either an input or output error that can be traced to a single station. |
| Hard Errors - Beacons | a beacon. The equivalent of a ring reset, a beacon indicates a serious problem and can bring the ring down. There are two types of beacon: input and output. |


For more about soft and hard errors, see About Soft Errors on page 14-10, and About Hard Errors on page 14-10. Beacons are explained further in Understanding and Viewing Errors on page 14-10.



## 14.1.3 Selecting Active Stations Only

You may want to see data only for *active* stations—stations currently on ring. If a station was on the ring at some point, but is now *off*, it is referred to as inactive. To view only the active stations on the ring, use the following procedure.

1. Select the View menu.
2. Click on Active Stations Only.

The list box updates the display to show only the active stations on the ring.

## 14.1.4 Sorting List Box Information

You can change the way *ForeView RMON **ST*** sorts the information provided in the window's list box. You can use any of these variables to determine the sort order:

- **Ring Order.** The position of the station in the ring. The default variable.
- **MAC Order**. MAC addresses in descending order.

- **Enter Time**. The last time the station has entered the Ring. The sort is in descending order.
- **Exit Time**. The last time the station has exited the Ring. The sort is in descending order.
- **Hard Errors**. (Summary window only.) Sums the two types of hard errors for the station, In and Out, and sorts in descending order. See Understanding and Viewing Errors on page 14-10.
- **Soft Errors.** (Summary window only.) Sums the three types of soft errors for the station, In, Out, and Non (non-isolating), and sorts them in descending order. For more information, see the discussion of errors on page 3-10.

You can use the following procedure to change the list box sort order.

1. Select Sort from the menu bar.
2. Click on the sort order variable you want.

The window is displayed with values sorted according to the variable you selected.

### 14.1.5 Refreshing the Station Information

You can refresh the station list box information to display the most recent data. Click on the Refresh button, or select Tools/Refresh from the menu bar, and *ForeView RMON **ST*** updates the list box data.

## 14.2 Viewing Station Configuration

Ring Monitor's View Config function lets you see a selected station's group address, MAC address, last update time, and functional address. To view a station's configuration, use the following procedure.

1. Select the appropriate agent from the *ForeView RMON **ST*** main window.
2. Select the Ring Monitor icon in the *ForeView RMON **ST*** main window.
   The Ring Monitor Station List window is displayed.
3. Click on the View Config button or select Tools/View Config from the menu bar.
   The Station Configuration window is displayed as shown in Figure 14.3.


**Figure 14.3 -** Station Configuration window



4. You can update the configuration information for this station at any time. To do so, select the Update button from the Station Configuration window. The agent gets the latest configuration from the station. To see the latest update, again click on View Config from the Ring Monitor window.
5. Click on OK when you're finished viewing the station configuration.

## 14.2.1 Viewing Host Information

You can launch *ForeView RMON **ST***'s Host List from both the Ring Station List window, and from the Source Routing Monitor application, explained in Using Source Routing Monitor to see Inter- and Intra-Ring Traffic on page 14-12.

You can use Host List to view a complete list of the hosts and host activity detected by the selected Token Ring agent. (See Chapter 7 for more information on the Host List tool.) You can use Host list to verify the number of hosts in a domain, or that a host is included in a particular domain.

To launch Host List from the Ring Station List window, or from the Source Routing Monitor main display, click on the Host List button, or select Tools/Host List from the menu bar. Figure 14.4 displays the Host List main window.

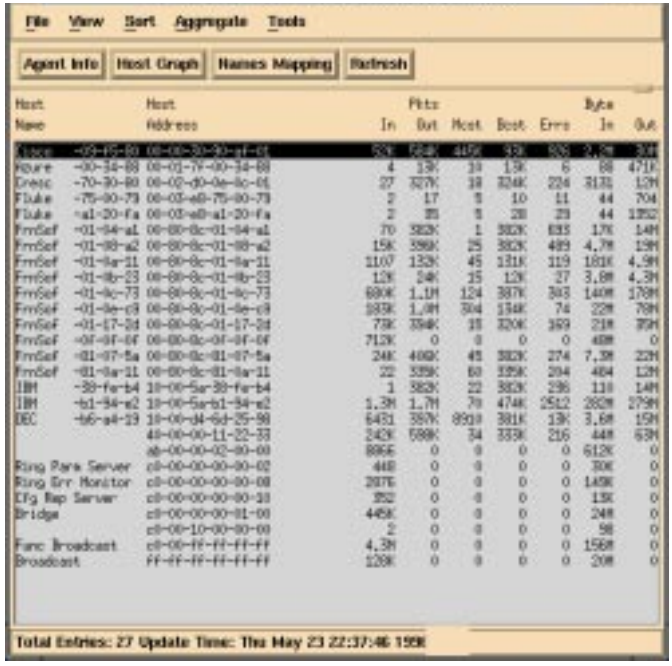



**Figure 14.4 -** *ForeView RMON **ST*** RMON Host List window

You can now work with the Host List application as described in Chapter 7: Monitoring and Troubleshooting Single Domains.

## 14.2.2 Removing a Station from the Token Ring

You can remove a station from the Token Ring using Ring Monitor. To remove a station from the Token Ring, use the following procedure.


This procedure removes the selected station from the token ring. Use the Tools/Remove command with extreme caution.

1. Select the station you want to remove by highlighting it in the list box.
2. Click on the Remove button, or select Tools/Remove from the menu bar. A cautionary dialog box prompts you to confirm that you really want to remove the station.

3. Click on OK to remove the station, or Cancel to quit without removing the station.

## 14.2.3 Printing the Contents of the List Box

You may want to print the contents of the Ring Monitor list box (in either status or summary view) for future reference.

To print the contents of the list box, use the following procedure.

1. Select the Print menu. The Print Options box is displayed as shown in Figure 14.5.


**Figure 14.5 -** Print Options box

2. Do one of the following:
   - To print the list box information to a file, select File as the destination, specify the directory path under **Directory**, and type the filename in the **File** field.
     *or*
   - To print directly to a printer, select Printer as the destination, and type the printer name in the **Printer** field.
3. Click on Apply.

To exit Ring Monitor, select File/Exit from the menu bar.

# 14.3 Understanding and Viewing Errors

This section contains a brief discussion of Token Ring errors. See the applicable Token Ring reference manuals for a complete explanation.

*ForeView RMON **ST*** registers two types of Token Ring errors: soft errors and hard errors. There are other Token Ring errors, but this section covers only those that *ForeView RMON **ST*** uses.

## 14.3.1 About Soft Errors

A soft error is an error that occurs during normal ring operation. It does not cause the ring to come down. There are two types of soft errors: isolating and non-isolating.

### 14.3.1.1 Isolating Errors

An isolating error is a soft error that can be traced to a single station. There are two types of isolating soft errors:

- **Input.** An input isolating error is calculated by summing Line Errors plus Burst Errors. Input isolating errors usually indicate a problem with the station's NAUN.
- **Output.** An output isolating error is calculated by summing Line Errors, Burst Errors, Internal Errors, AC, and Abort Errors. Output isolation errors usually indicate a problem with the station itself.

### 14.3.1.2 Non-isolating Errors

A non-isolating error is a soft error that cannot be isolated to a single station. A non-isolating error is calculated by summing Lost Frames, Congestion, Frame Copied, Token, and Frequency Errors. Non-isolating errors do not indicate a problem with a particular station but, rather, with the ring itself.

## 14.3.2 About Hard Errors

A hard error is the equivalent of a system reset. It is a serious error that can bring the ring down. Hard errors are specific to a single station on the ring. There are two types of hard errors:

- **Input.** The number of beacon frames sent.
- **Output.** The number of beacon frames with this station as NAUN.

## 14.3.3 Viewing Errors

There are two ways to view Token Ring errors:

- You can view a summarized list of errors in the Summary View section of the Ring Monitor window. You obtain this view by selecting Summary from the View menu in the Ring Station List window.
- You can view a detailed list of errors for a particular station.

To view a detailed list of errors for a particular station, use the following procedure.

1. Select the appropriate agent from the *ForeView RMON* ***ST*** main window.
2. Click on the Ring Monitor icon from the *ForeView RMON* ***ST*** main window. The Ring Monitor Station List window is displayed.
3. Select the station for which you want to see errors, from the list box in the Ring Monitor window.
4. Click on the View Errors button. The Station Statistics window is displayed. This window lists Ring Station information, soft errors, and hard errors under corresponding headings. Figure 14.6 shows the Station Statistics window with errors displayed.


**Figure 14.6 -** Station Statistics window (errors displayed)

5. Click on OK when you're finished viewing the station statistics.

## 14.4 Using Source Routing Monitor to see Inter- and Intra-Ring Traffic

You can see a detailed summary of traffic passing both in and out of the ring, as well as traffic within the ring, using the Source Routing Monitor. To use the Source Routing Monitor to view a summary of ring traffic, use the following procedure.

1. Select the appropriate agent from the *ForeView RMON **ST*** main window.
2. Click on the Ring Monitor icon from the *ForeView RMON **ST*** main window. The Ring Monitor Station List window is displayed.
3. In the Ring Monitor window, select the station for which you want a traffic summary.
4. Click on the SR Monitor button or select Tools/SR Monitor from the menu. Figure 14.7 shows the Source Routing Monitor window.

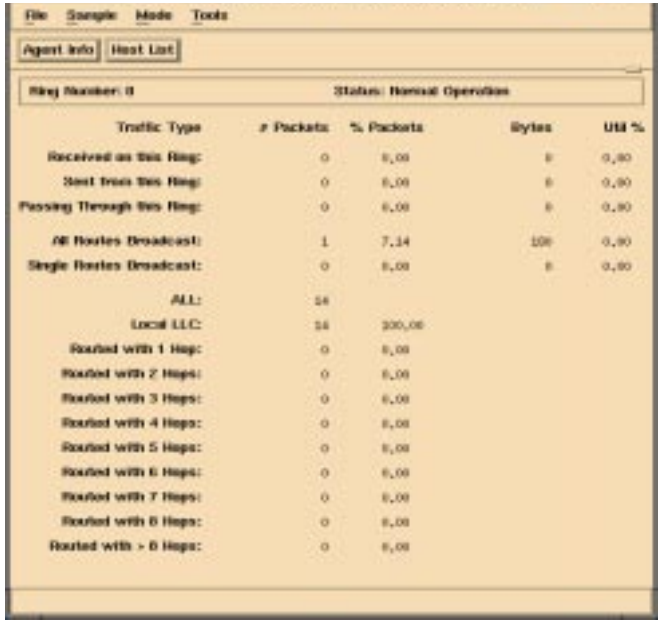



**Figure 14.7 -** Source Routing Monitor window

## 14.4.1 Selecting the Sample Interval

You can select the sample interval, which is how long *ForeView RMON **ST*** waits before polling the agent and updating the display with the new ring information. The range is from 15 seconds to 5 minutes. To select the sample interval, use the following procedure.

1. Select Sample from the menu bar.
2. Click on the sample interval you want.

## 14.4.2 Getting Agent Information

You can get system and interface information on the selected agent directly from the Source Routing Monitor window. To do so, use the following procedure:

1. Click on the Agent Info button, or select Tools/Agent Info from the menu bar to view the Agent Information window. The Agent Information window is shown in Figure 14.1.


**Figure 14.8 -** Agent Information window

2. Click on OK when you're finished viewing the agent information.

## 14.4.3 Printing Source Routing Information

You may want to print the contents of the Source Monitor window for future reference. To do so, follow the procedure outlined in Printing the Contents of the List Box on page 14-9.

To exit the Source Routing Monitor at any time, select File/Exit from the menu bar.

# CHAPTER 15 Monitoring FDDI Networks with Ring Monitor



Station Management (SMT) is the layer of the FDDI protocol that is responsible for monitoring network operation, detecting errors, and isolating faults. SMT initializes nodes, inserts nodes to the ring, and removes nodes from the ring.

Each FDDI node participates in ring management by exchanging SMT information (using SMT frames) with other nodes on the ring. There are different types of SMT frames, each used for a specific purpose. For example, SMT Status Report Frames are sent wherever there is a change in the ring configuration. Similarly, SMT NIFs (Neighbor Information Frames) are used by FDDI nodes to determine or announce their neighbors. These SMT NIF frames contain the address of the sender, the address of its nearest upstream neighbor, and additional information about the node itself. By capturing and analyzing these frames, Ring Monitor can build a map of the ring. You use Ring Monitor to configure, display, and print FDDI statistics.


Not all network probes can be configured to monitor SMT NIF frames. Check your network probe documentation to ensure that SMT NIF frames are supported before attempting to configure Ring Monitor.

For more detailed information about configuring Ring Monitor to gather FDDI statistics, see the following sections:

## 15.1 Building the Ring Map

Ring Monitor builds a ring map by collecting SMT Neighbor Information Frames (SMT-NIFs). These SMT frames are exchanged periodically, in intervals between 2-30 seconds. When the FDDI ring monitor application is launched, the FDDI network probe starts collecting the SMT-NIFs and building the FDDI ring map.

However, the ring map is complete only when the probe has been able to collect SMT-NIFs from all the nodes on the ring. Until that happens, a partial ring map is displayed and the Ring Map Status in the Ring Monitor is displayed as Incomplete. When the ring map is complete (typically, 10-60 seconds), the Ring Map Status is displayed as Complete. Note that the ring map is rebuilt whenever there is a change in the ring configuration.

Although the time taken to build the ring map is typically less than 60 seconds, under certain conditions, the ring map may take longer to be completed, or may never be completed at all. If the ring is overloaded, the nodes take longer (several minutes) to exchange SMT-NIFs. Therefore, the time to build the ring map increases as well. If there a node on the ring that has stopped, or there is a node that does not exchange SMT-NIFs, the ring map will never be completed. A node will stop exchanging SMT-NIFs if it has hung, is too busy to participate in the SMT-Neighbor Protocol, or if it does not conform to the SMT-NIF protocol.

## 15.2 Viewing The Ring Station List for an FDDI Agent

Use the following procedure to launch Ring Monitor from the *ForeView RMON **ST*** main window and display Ring Monitor's Ring Station List for the FDDI agent you select.

1. Log in to the network management station where *ForeView RMON **ST*** is installed, and run the *ForeView RMON **ST*** application.
2. Select an FDDI agent from those shown in the Agents[All] list box or select the agent group containing the FDDI agent you want to monitor. If the agent you want is not listed, you may need to add it. See Chapter 4 for more information on adding Agents.
3. Click on the Ring Monitor icon, or select Application/Ring Monitor from the menu bar to access the Ring Station List.

Figure 15.1 shows the Ring Monitor's main window. The Ring Station List is displayed for the selected agent. From this main window, you can now work with Ring Monitor in a variety of ways, described by various procedures in this chapter.



**Figure 15.1 -** Ring Station List window (FDDI network)

## 15.2.1 The Ring Station List Upper List Box Display

The Ring Station List window consists of an upper list box and a lower list box. The upper list box shows information about each of the nodes on the ring, and contains the following information:

- **Ring Order.** The order of this station in the ring.
- **Station.** The name of the station.
- **Address.** The address of the station.
- **Last Enter Time.** The last time the station entered the ring.
- **Last Exit Time.** The last time the station exited the ring.
- **RIns.** Ring insertions. The number of times a station has been inserted into the ring.
- **Status.** Whether a station is active (currently in the ring) or inactive (not currently in the ring).

## 15.2.2 The Ring Station List Lower List Box Display

The lower list box shows information about the specific node highlighted in the upper list box. It contains the following information:

- **Station Address.** The name and address of the highlighted station.
- **Nearest Upstream Neighbor Address.** The address of the nearest active upstream neighbor (NAUN) of the highlighted station.
- **Node Class.** FDDI nodes can be classified into Stations and Concentrators. The primary purpose of a Station is to transmit and receive information. Concentrators are like hubs, providing facilities to connect additional Nodes. Some types of Nodes can have zero, one, or two MAC addresses. For example, a Dual Attachment Node with two MAC addresses is able to simultaneously receive and transmit frames on both the logical rings. This is not possible with a Dual Attachment Node that has only one MAC. Node Class indicates the node type and can be any one of the following:
  - Single Attachment Station (SAS).
  - Single MAC - Dual Attachment Station (SM-DAS).
  - Dual MAC - Dual Attachment Station (DM-DAS).
  - MACless - Single Attachment Concentrator (SAC).
  - Single MAC - Single Attachment Concentrator (SAC).
  - Single MAC - Dual Attachment Concentrator (DAC).
  - Dual MAC - Dual Attachment Concentrator (DAC).

- **Topology State.** The topology state of the node indicates whether it is correctly connected on the ring. The states are indicated as follows:
  - **Normal**. The node is correctly connected.
  - **Twisted Ring A-A.** In case of a Dual Attachment Node, the A-port should be connected to the B-port of its Upstream Neighbor and the B-port should be connected to the A-port of its Downstream neighbor (except if *Dual Homing* is used). Connecting the A-port of Dual Attachment Node to the A-port of another Dual Attachment Node results in a topology that is referred to as a twisted ring.
  - **Twisted Ring B-B.** This is similar to the Twisted Ring A-A topology explained above, except that it's caused by connecting the B-port of a Dual Attachment Node to the B-port of another Dual Attachment Node.
  - **Wrap.** FDDI defines a *redundant* topology network. If a fault occurs on the trunk ring, then the Dual Attachment Nodes on either side of the faulty link wrap around to bypass the faulty link. These nodes are then said to be in a *wrapped* state.

  The following information indicates how the node is connected to the FDDI ring:
  - **Rooted Station/Station not Rooted.** Displayed if the node is a Station. A Station is *rooted* if it does not have an active A, B, or S port in tree mode. This indicates whether the station is directly connected on the trunk ring *(rooted*), or if it is connected through a concentrator as part of a tree topology (*unrooted*).
  - **Attached Concentrator/Unattached Concentrator**. Displayed if the node is a Concentrator.
  - **UnAttached Concentrator.** Displayed if the node is a Concentrator. A Concentrator is *UnAttached* if it does not have an active A, B, or S Port. In an FDDI dual-ring topology or a dual-ring with trees topology, all concentrators are normally *Attached*. In an FDDI tree topology, any number of concentrators are arranged in a hierarchy, with a number of stations attached to each concentrator. In this topology one concentrator is the root of the tree. This concentrator is *UnAttached*. All other concentrators are *Attached* under normal conditions.
- **Synchronous Service.** FDDI allows for two different types of traffic, synchronous and asynchronous. *Synchronous* traffic consists of delay-sensitive traffic such as voice packets, which need to be transmitted within a certain time interval. *Asynchronous traffic* consists of data traffic produced by various computer communication applications, such as file transfer, and mail, among others. These data packets can sustain some reasonable delay.

  If the node supports synchronous traffic then the following is displayed:

```
Synchronous Service: Supported
```

If it does not support Synchronous traffic, then the following is displayed:

```
Synchronous Service: Not Supported
```

- **Duplicate MAC Address Test.** On an operational FDDI ring, each node periodically checks to see if any other node on the ring has the same MAC Address as its own. If a duplicate MAC Address condition does not exist, then the following is displayed:

```
Duplicate MAC Address test: Passed
```

If not, then either of the following is displayed:

```
Duplicate MAC Address test: Failed (My duplicate exists).
Duplicate MAC Address test: Failed (My Upstream is duplicate).
```

## 15.2.3 Selecting Active Stations Only

You can view data on active stations. To do so, use the following procedure.

1. Select the View menu.
2. Click on Active Stations Only.

## 15.2.4 Sorting List Box Information

You can change the way *ForeView RMON **ST*** sorts the information provided in the window's list box by selecting Sort from the menu bar, then selecting one of the following:

- **Ring Order.** The position of the station in the ring. This is the default setting.
- **MAC Order**. MAC addresses, sorted in descending order.
- **Enter Time**. The last time the station has entered the Ring, sorted in descending order.
- **Exit Time**. The last time the station has exited the Ring, sorted in descending order.

### 15.2.5 Refreshing Station Information

To refresh the station list box information to display the most recent data, click on the Refresh button in the Ring Monitor window. *ForeView RMON **ST*** updates the list box data.

## 15.3 Viewing Host Information



You can launch *ForeView RMON **ST***'s Host List from the Ring Station List window to view a complete list of the hosts and host activity detected by the selected FDDI agent. You may use Host List to verify the number of hosts in a domain, or simply that a host is included in a particular domain.

To launch Host List from the Ring Station List window, click on the Host List button, or select Tools/Host List from the menu bar. When you do so, the Host List main window is displayed as shown in Figure 15.2.


**Figure 15.2 -** *ForeView RMON **ST*** Host List window

You can now work with the Host List application as described in Chapter 7: Monitoring and Troubleshooting Single Domains.

## 15.4 Printing the Contents of the List Box

You may want to print the contents of the Ring Monitor list box for future reference. To print the contents of the list box, use the following procedure.

1. Select File/Print from the menu bar to access the Print Options box as shown in Figure 15.3.


**Figure 15.3 -** Print Options box

2. Do one of the following:
   - To print the list box information to a file, select File as the destination, specify the directory path under **Directory**, and type the filename in the **File** field.
     *or*
   - To print directly to a printer, select Printer as the destination, and type the printer name in the **Printer** field.
3. Click on Apply.

To exit Ring Monitor, select File/Exit from the Ring Monitor main window.

# CHAPTER 16 Customizing Filters and Domains



*ForeView RMON* ***ST*** is shipped with the capability to respond to most network management needs. However, you can customize *ForeView RMON* ***ST*** to conform to your specific network management requirements. The two primary tools you can use to customize *ForeView RMON* ***ST*** are Filter Editor and Domain Editor.

Before you start a data capture session or create a custom domain, you need to decide the type and extent of the data to collect for display and analysis. You select an appropriate filter to screen the incoming data when you start a data capture session or create a custom domain.

For more detailed information on the customizing the Filters and Domains, see the following sections:



## 16.1 *ForeView RMON ST* Filter Editor Resources

*ForeView RMON* ***ST*** is shipped with a number of predefined filters. These filters should handle most data capture and domain requirements. If you need filtering parameters that aren't available in the existing filters, however, you can use Filter Editor to edit existing filters or create new filters that meet your requirements. You can view the list of available filters by running Domain Editor's Add function (see Defining New Domains on page 16-10).

To collect only selected data, you can create a set of filters that are either inclusive or exclusive, and that pass, capture, and store only the packets that meet the filter criteria. Filter creation begins with a filter format that uniquely describes the specific characteristics of the frame

which must be matched for acceptance or rejection of data packets from the data capture buffers. Filter formats are based on the detailed structure of the seven-layer protocol stack that makes up a transmission frame.

*ForeView RMON **ST*** includes a substantial number of pre-established formats for the most commonly-used stacks. You can create new filters using these formats to explore a current problem, or define and store them for later use. To see a list of the filter formats that are available, use the Add function in the Filter Editor (For information on the Filter Editor, see Adding New Filter Definitions on page 16-5).

When you've created the appropriate filter, you insert it into the filter definition to be used for the data capture session. You can create highly selective filters that eliminate extra detail that may otherwise obscure the protocol decode process. The *ForeView RMON **ST*** Filter Editor offers the following four functions:

- Adding a new filter definition
- Editing an existing filter definition
- Viewing an existing filter definition
- Deleting an existing filter definition

## 16.2 Filter Types and Field Values

Before you get started adding or modifying filters, you need to be aware of the different ways you can specify field values. Values you can specify for a field in any given filter depend upon the type of filter format you select. As mentioned earlier, *ForeView RMON **ST*** includes many pre-established formats for the most commonly-used stacks. Once you select a filter format, the corresponding fields are displayed.

Except for the filter name, which is required, the remaining fields are all optional; you define only those fields that fit your needs. The fields you'll see may require a single-byte value, or multiple bytes. How you specify the values, for the most part, is up to you.

## 16.2.1 Understanding Filter Types

In *ForeView RMON **ST*** Filter Editor, you can choose from two filter types: physical or logical. The filter type depends upon the filter format you select. A physical format is topology-specific. This means that the filter criteria you define must be used with a specific media type, and is applied to frames at fixed positions. We recommend using a Token Ring-specific physical filter only on Token Ring topologies. *ForeView RMON **ST***'s predefined physical filters are:

- **SMT**. Use this filter *only* on FDDI networks.
- **TRMAC**. Use this filter *only* on Token Ring networks.
- **TRNONMAC**. Use this filter *only* on Token Ring networks.

A logical filter is one you can use on any network. This means that no matter the topology, *ForeView RMON **ST*** applies the criteria you specify at the appropriate position in a frame. These logical filters are useful because they can save you work. For example, if you need an IP filter to be applied on a Token Ring network as well as an Ethernet network, you can define one filter that works on both.




Each predefined filter format has a corresponding file. In these files, designated by the .ff extension, you'll find a listing of each optional field, its size, and its type, if applicable. Any time you need to know the number of bytes in a field, we recommend that you view the file.

## 16.2.2 Specifying Values when Defining Filters

In *ForeView RMON **ST***, when you specify values during filter definition, you can use different numeric styles: decimal, hexadecimal (hex), binary, or IP address format (dotted). The numeric style you use to specify values depends on two things: whether the field is single-byte or multi-byte, and whether the field is tied to a certain type, such as MAC address, which accepts only a hex value. To find out whether a field is single byte or multi-byte, you can open any predefined filter format file, contained in your usr/fore/foreview/fvrmon/usr directory. For example, if you wanted to find out how many bytes the Time-to-Live field requires in an IP filter format, you would go to your usr/fore/foreview/fvrmon/usr directory and type the following:

**cat ip.ff**

After pressing <Enter>, the filter format file (ip.ff) is displayed, showing all fields defined for the IP filter type, number of bytes required for each field, and any specific value type associated with a field (such as MACADDR, the MAC address type).

### 16.2.2.1 Guidelines for Working with Single-Byte Fields

In single-byte fields, you can specify the following numeric types, keeping in mind any restrictions as noted:

- **Hex**. Hex values must contain characters from the hex numeric set, **0-9** or **a-f**. However, if a hex value you specify is all numeric, *ForeView RMON **ST*** translates it as a decimal number. For example, if you're thinking in hex, and you want to specify **Time to Live** as **128** seconds, when you enter the hex value **80**, *ForeView RMON **ST*** translates the **Time to Live** field as **80** seconds, instead of the **128** you wanted.
- **Decimal**. Decimal values must contain all numbers and *no* dots. This means that if you want to specify **Time to Live** as **128** seconds, you'll enter **128**, not **128.00**. If you *do* enter **128.00**, *ForeView RMON **ST*** translates your entry as a two-byte value and displays an error message advising you that **Time to Live** is a single-byte field.
- **Binary**. Binary numbers, which are only 0s and 1s, *must* begin with capital **B**.
- **Wildcards**. There are two acceptable wildcards you can specify when you only want to specify part of a numeric value. When you're specifying hex or decimal numbers, you can specify an uppercase **X** as a wildcard (careful, it's case-sensitive). This uppercase **X** is a placeholder for one byte of information for decimal values, or four bits for hex values. However, if you're working with binary numbers, you must use a lowercase **x** as a wildcard (again, it's case-sensitive). This lowercase **x** is a placeholder for one bit of information.

### 16.2.2.2 Guidelines for Working with Multiple-Byte Fields

In multiple-byte fields, you can specify the following numeric types, keeping in mind any restrictions as noted:

- **Hex**. Hex values must contain characters from the hex numeric set, **0-9** or **a-f**. However, if a hex value you specify is all numeric, *ForeView RMON **ST*** translates it as a decimal number.
- **Decimal**. Decimal values in multiple-byte fields can contain numbers and dots. Keep in mind, however, that *ForeView RMON **ST*** reads each side of a dot as a separate number. This means that if you specify a number as **255.255.255.75**, *ForeView RMON **ST*** reads four values: **255, 255, 255,** and **75**.
- **Binary**. Binary numbers, which are only 0s and 1s, *must* begin with capital **B**.
- **Wildcards**. There are two acceptable wildcards you can specify when you only want to specify part of a numeric value. When you're specifying hex or decimal numbers, you can specify an uppercase **X** as a wildcard (careful, it's case-sensitive). This uppercase **X** is a placeholder for one byte of information for decimal values, or four bits for hex values. However, if you're working with binary num-

bers, you must use a lowercase **x** as a wildcard (again, it's case-sensitive). This lowercase **x** is a placeholder for one bit of information.

- **Binary & hex combination**. In *ForeView RMON **ST***, you can use a combination of binary and hex values in any multi-byte field. This is especially useful when you want to capture multicast packets on different network topologies.

## 16.3 Adding New Filter Definitions



When you're ready to add a new filter, use the following procedure.

1. Click on the Filter Editor icon from the *ForeView RMON **ST*** main window, or select Tools/Filter Editor from the menu bar to access the Filter Editor window, shown in Figure 16.1.

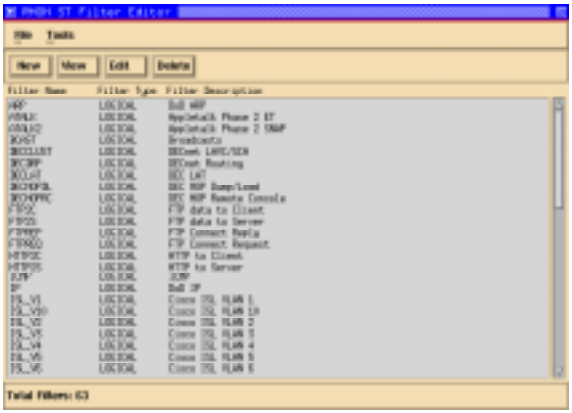


**Figure 16.1 -** Filter Editor window

2. Click on New. The New Filter window is displayed (see Figure 16.2 on page 16-6). Most of the window shows blank rectangles, which are used later to designate fields for a specified filter format, as described in Step 4.

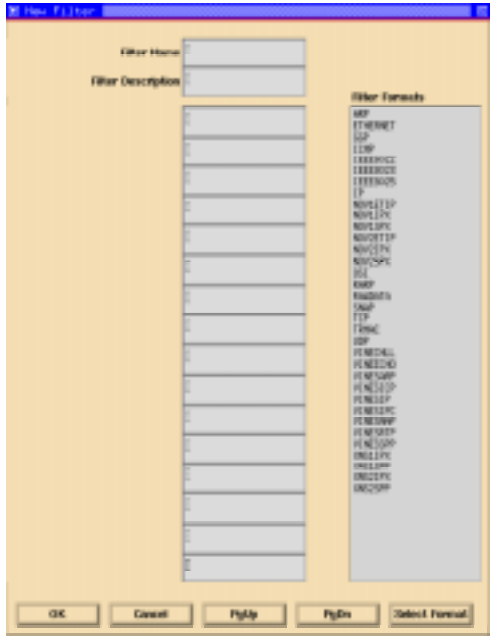



**Figure 16.2 -** New Filter window

3. Enter a name for the new filter in the Filter Name field by specifying up to 8 letters, numbers, dashes, or underscores. Keep in mind that the name must begin with a letter, and *is* case-sensitive.
4. To select a format for the new filter, highlight the format you want from those listed in the **Filter Formats** list box. Then click on Select Format.

   The New Filter window changes its display. Instead of a column of blank rectangles, now field names are displayed. Depending on the filter format selected, only three fields or two pages may be displayed. For example, if you selected the TCP filter format, the New Filter window displays field names for all the rectangles shown in the window, and the PgDn button is enabled. This means you can click on this button to see the rest of the fields available for defining the filter. Then click on the PgUp button to toggle back to the first page of the window.
5. For certain filters, some fields already contain values. Fill in additional fields as needed.
6. Click on OK to add the filter. The filter is now displayed in the filter list.

## 16.4 Editing Filter Definitions

To edit an existing filter definition, use the following procedure.

1. Click on the Filter Editor icon from the *ForeView RMON **ST*** main window, or select Tools/Filter Editor from the menu bar to access the Filter Editor window. Figure 16.1 on page 16-5 shows the Filter Editor window.
2. Select the filter you want to edit from the filter list in the Filter Editor window by highlighting it.
3. Click on Edit to access the Edit Filter window. This window, shown in Figure 16.3 on page 16-8, is the same as the New Filter window, except that existing fields are already filled in with the values you last specified.


You can use the Edit Filter window as a shortcut to create a new filter with characteristics similar to an existing filter. Just edit the fields that are different, change the filter name, and save it.

**Figure 16.3 -** Edit Filter window

4. Change the fields you want to edit.
5. Click on OK to create the new filter or Cancel to quit.

## 16.5 Viewing Filter Definitions

Before using a filter in the Data Capture tool, or creating a new filter, you can look at the field definitions for one or more existing filters. You can view the field definitions for an existing filter without changing any filter information. To see existing filter definitions, use the following procedure.

1. Click on the Filter Editor icon from the *ForeView RMON **ST*** main window, or select Tools/Filter Editor from the menu bar.

   The Filter Editor window is displayed as shown in Figure 16.1.
2. Select the filter you want to view from the filter list in the Filter Editor window by highlighting it.

3. Click on View to display the View Filter window. This window is the same as the Edit Filter window shown in Figure 16.3 on page 16-8, but you cannot change any fields.
   If applicable, click on PGDn or PgUp to scroll through all the fields containing values for the filter you're viewing.
4. Click on Cancel when you are finished viewing the filter.

## 16.6 Deleting a Filter Definition



When you no longer need a filter, you can delete the filter definition to conserve system resources. The Filter Editor window is displayed as shown in Figure 16.1. To delete a filter definition from the filter list, use the following procedure.

1. Click on the Filter Editor icon from the *ForeView RMON **ST*** main window, or select Tools/Filter Editor from the menu bar.
2. Select the filter you want to delete from the filter list in the Filter Editor window.
3. Click on Delete. A cautionary window is displayed that prompts you to confirm that you really want to delete the filter.
4. Click on OK to delete the filter definition, or Cancel to quit without deleting the filter definition.

You can exit Filter Editor at any time by selecting File/Exit from the menu bar.

## 16.7 *ForeView RMON ST* Domain Editor Resources

*ForeView RMON **ST*** is shipped with a number of standard domains already defined. These domains let you monitor most types of network traffic. If these are not sufficient, you can use the Domain Editor tool to create new domains or edit existing domains to meet your monitoring needs. You can choose to create generic or protocol-specific domains in *ForeView RMON **ST***.

When you define a domain, you determine the subset of network traffic that the domain represents. Once you define a domain, you can install it on one or more agents and monitor that portion of network traffic.

In this section, you'll learn how to define new domains, modify existing domains to meet new monitoring requirements, and delete domains when you no longer need them.

# 16.8 Defining New Domains

The Domain Editor lets you add, edit, or delete generic or protocol-specific domain definitions. When a domain is defined, you can attach it to one or more agents. *ForeView RMON **ST*** is shipped with a number of predefined domains. However, you can define a custom domain to monitor a specific subset of traffic on your network.

## 16.8.1 Defining Protocol Domains

To define a new protocol domain, use the following procedure. Keep in mind that after defining a new domain, you need to add it on an agent for it to be useful. For more information about Domain Manager and adding domains on an agent, see Chapter 6: Working with Domains and Domain Manager. The Domain Editor window is displayed as shown in Figure 16.4.

1. Click on the Domain Editor icon from the *ForeView RMON **ST*** main window or select Tools/Domain Editor from the menu bar.

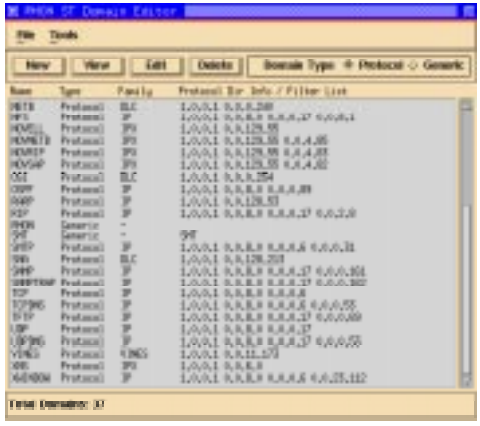


**Figure 16.4 -** Domain Editor window

2. To the right of the **Domain Type** field, select Protocol.
3. Click on the New button to access the New Protocol Domain window, shown in Figure 16.5 on page 16-11.

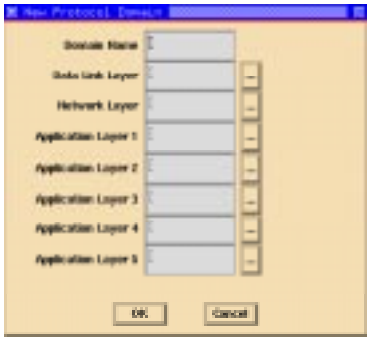


**Figure 16.5 -** New Protocol Domain window

4. In the **Domain Name** field, type the name you want associated with the domain you're defining. This can be a maximum of 15 characters and must begin with a letter. You can use only letters, numbers, dashes, and underscores. The name is not case sensitive
5. To the right of the **Data Link Layer** field, click on the selection button. When you do so, a list of supported network topologies (media) is displayed. You can choose from Ethernet, Token Ring, FDDI, and WAN.
6. To the right of the **Network Layer** field, click on the selection button. A list of parent protocols is displayed. Parent protocols are high level protocols. The list shows the protocol name, as well as a number that maps to an RMON2 definition. The protocols you see are those that work on the media type you selected in Step 5.
7. Select the protocols you want to include as part of the domain you're defining.
8. For any of the **Application Layer** fields 1 through 5, click on the selection button to the right of each field you want to define. Keep in mind that all these fields are optional, which means that you can define none of these fields, or as many as all five.

**NOTE**

For each selection button you click on, a list of protocol children is displayed. Children protocols are those that are related to the protocols you selected in Step 6. You can choose to examine multiple children protocols running on a level above selected parent protocols. The list shows the children protocol name, as well as a number that maps to an RMON2 definition.

9. Select any children protocols you want to include as part of the domain you're defining.
10. When you've finished defining the domain, click on OK to save your choices, or Cancel to close the window without saving your definition.

## 16.8.2 Defining Generic Domains

You can define generic domains only on NETscout Probes. To define a new generic domain, use the following procedure. Keep in mind that after defining a new domain, you need to add it on an agent for it to be useful. For more information about Domain Manager and adding domains on an agent, see Chapter 6: Working with Domains and Domain Manager.

1. Click on the Domain Editor icon from the *ForeView RMON **ST*** main window or select Tools/Domain Editor from the menu bar. The Domain Editor window is displayed as shown in Figure 16.4 on page 16-10.
2. To the right of the **Domain Type** field, select Generic.
3. Click on the New button. The New Generic Domain window is displayed as shown in Figure 16.6.

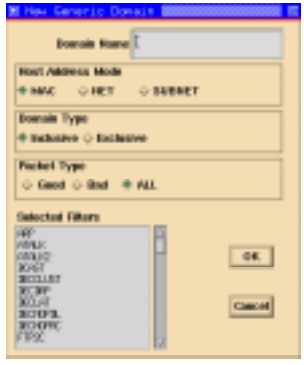



**Figure 16.6 -** New Generic Domain window

4. In the **Domain Name** field, enter the name of the domain as you want it displayed throughout *ForeView RMON **ST***. The name can be a maximum of 15 characters and must begin with a letter. You can use only letters, numbers, dashes, and underscores. The name is not case sensitive.
5. Under the **Host Address Mode** heading, select how you want host addresses displayed: MAC, NET, or SUBNET.

6. Under the **Domain Type** heading, select one of the following:
   - Inclusive. The default value. Choosing this type means that a packet is accepted into the domain if it matches any of the filters.
   - Exclusive. Choosing this type means that a packet is accepted into the domain if it fails to match all of the filters.
7. Under the **Packet Type** heading, select one of the following:
   - Good. Selects only good packets as part of the domain.
   - Bad. Selects only bad packets as part of the domain.
   - All. The default value. Selects all packets as part of the domain.
8. Under the **Selected Filters** heading, scroll down and select one or more (up to 8) filters you want to include as part of the generic domain you're defining. You can mix and match any of the network layer protocols displayed. The filters you select determine the type of packets the new generic domain recognizes as follows:
   - If you selected Inclusive, these are the packets the domain passes.
     *or*
   - If you selected Exclusive, these are the packets the domain rejects.
9. Click on OK to define the new generic domain with your choices, or click on Cancel to close the window without saving your choices in a new generic domain definition.



## 16.9 Editing or Viewing an Existing Domain Definition

You can change a domain's definition when you want to monitor a different subset of network traffic. You also can use the Edit Domain function to create a new domain by modifying an existing domain, and then renaming it. You can view the parameters of an existing domain without editing it. You can also edit a previously defined domain whether it is attached to an agent or not. To change or view the information for an existing domain, use the following procedure:

1. Select the domain you want to edit from the Agent Summary area in the Domain Editor window.
2. Click on Edit or View from the Domain Editor window. Depending on the type of protocol you selected, one of the following is displayed (keep in mind that each window corresponds to the Add window, except that fields are already filled with values you specified earlier).

- If you selected a protocol domain and clicked on Edit, the Edit Protocol Domain window is displayed as shown in Figure 16.7.

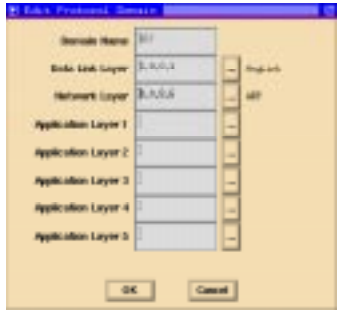


**Figure 16.7 -** Edit Protocol Domain window

*or*

- If you selected a generic domain and clicked on Edit, the Edit Generic Domain window is displayed as shown in Figure 16.8.

**Figure 16.8 -** Edit Generic Domain window

- If you selected a protocol domain and clicked on View, the View Protocol Domain window is displayed. The View Protocol Domain window is the same as the Edit Protocol Domain window shown in Figure 16.7, but the fields cannot be modified.
  *or*
- If you selected a generic domain and clicked on View, the View Generic Domain window is displayed. The View Generic Domain window is the same as the Edit Generic Domain window, but the fields cannot be modified.

3. Do one of the following:
   - If you selected Edit, change the fields you want to modify.
     *or*
   - If you selected View, you can view the window but not make any changes.


If you're editing either a generic or protocol domain, turn back to the sections describing how to define each for information on what you can modify. For protocol domains, see page 3-10. For generic domains, see page 3-12.

4. Do one of the following:
   - If you **edited** a domain, either click on OK to modify the domain, or Cancel to return to the Domain Manager window without saving your changes.
     *or*
   - **If you viewed** a domain, click on Cancel to close the domain window and return to the Domain Manager window.



## 16.10 Deleting a Domain Definition

When you no longer need to monitor the subset of network traffic defined by a domain, you can delete the domain definition to save resources. To delete a domain definition from *ForeView RMON **ST***:

1. Select the domain you want to delete from the Agent Summary list box in the Domain Editor window.
2. Click on Delete from the Domain Editor window. A cautionary prompt appears, asking if you want to continue.
3. Click on OK to delete the domain definition, or Cancel to return to the Domain Editor window.

To exit Domain Editor at any time, select File/Exit from the menu bar.

# PART 3 Appendices

This part contains reference information on the *ForeView RMON **ST*** Manager software.

This part contains the following appendices:

**APPENDIX A: Startup and Configuration Files**

**APPENDIX B: Error Messages**

**APPENDIX C: Assigned Numbers**

**APPENDIX D: NETscout Probe Applications**

# APPENDIX A Startup and Configuration Files

In this appendix, you'll find information on the agent startup file and alert script files. Basically, the agent startup script file contains information that you enter and modify that reflects the configuration of a specific probe. The alert script files contain information about various thresholds set on certain variables that you set through Trap Manager.

These two types of files are helpful when you need to reconfigure a probe that's been reset. For example, if you reboot the probe for any reason, you'll need to reconfigure the probe. To easily do so, you can run the startup file, which reinstalls all the domains and other parameters you'd specified on the probe and in the file. You can also run alert script files to reinstall trap conditions and thresholds that you want the probe to be aware of.

## A.1 Agent Startup File

When you define an agent by clicking the New button in the *ForeView RMON **ST*** main window, one of the fields is the name of the startup file. This field specifies the name of a script file to be executed when the configuration daemon (dvconfd) receives a configuration request from an agent that has been reset.

A default startup script file, named **startup**, ships with *ForeView RMON **ST***. The default path is $NSHOME/usr. This standard startup file is displayed as follows:

```
#
# Default startup script file "startup"
#
# Note: "$1" is a macro replaced by the agent name.

#
# Startup scripts must have execute permission.
#
```




The $NSHOME/usr path is set by the fvrmon script when you launch *ForeView RMON **ST***. When you are accessing any files from the command line, the path is usr/fore/foreview/fvrmon/usr.

The agent name is passed as an argument so that you can use the same startup script for multiple agents if you want. Typically, you use the startup script to configure or reconfigure an agent to a specific domain setup. The default startup does this by running the **dvinst** utility. The arguments passed to **dvinst** are the name of a configuration file, dvinst.cfg**,** and the name of the agent. The default dvinst.cfg (in $NSHOME/usr**)** is displayed below.

```
#
# Domain configuration file
#
#         Host     Segment   Short    Long
#Domain   Mode     Stats     History  History   Host    Conversation
#---------------- ------   ------- -------   ------- ---- ------------
RMON      MAC        y        y         y        y         n
```

## A.2 Alert Scripts

When you configure an alert at an agent using Trap Manager, you can specify the name of a script file to be executed when *ForeView RMON* ***ST*** receives a trap message from the agent. You can specify different scripts for rising and falling thresholds, as well as for different watched variables.

When the trap daemon (dvtrapd) receives a trap message from the agent, if the message specifies a script, the daemon executes it. The name of the agent and the user-specified severity level are passed as arguments to the script. An example alert script is displayed below.

```
#
# Sample alert script "mytrap.sh".
#
                              date > mytrap.$$
echo Trap received from agent $1, severity level $2.>>mytrap.$$

$NSHOME/bin/dvsnap $1 ALL HOST 15 10 >> mytrap.$$
mail `whoami` < mytrap.$$
```

Note that the **$$** macro is interpreted as the process ID, and **$1** and **$2** are the agent name and severity level, respectively. These are shell substitutions. The shell script should be given "execute" permission, for example:

**% chmod 755 mytrap.sh**

In this example, the script sends you a mail message indicating the time when the trap was received, the agent name and severity level, and a list of the top ten transmitting hosts for the fifteen-second interval following trap reception. From the script, you can run any of the *ForeView RMON **ST*** command line tools or other standard tools.

## A.3 Configuration Files



Configuration files contain definitions or parameters. Usually, you can edit configuration files to update information or further customize information for your organization's needs. Some configuration files are specific to a particular installation while others can be used at any installation. When a file is specific to a particular installation, it contains definitions that apply, usually, to hardware connected to segments local to where *ForeView RMON **ST*** is installed. The agent.lst file is an example; unique agent definitions and IP addresses apply only to agents on specific segments. All the configuration files described in this section are stored in the "configuration database." This database is also called the NSHOME/usr directory.

For example, if you had two *ForeView RMON **ST*** clients installed, one on a workstation in Paris, Texas, and the other in New York City, New York, you'd need a different agent.lst file for each *ForeView RMON **ST*** client. On the other hand, the domain.lst file contains domain definitions that you could use wherever *ForeView RMON **ST*** is installed. The following bulleted list outlines major configuration files available with *ForeView RMON **ST***.

- agent.lst. Specific to a particular installation, this file contains agent definitions. Each line within the file defines a unique SNMP agent that *ForeView RMON **ST*** can access. Agent names you specify can be up to 15 characters. You create and update this file through *ForeView RMON **ST***, although you can edit the file directly. You can define up to 1000 agents in this file.
- agegroup.lst. Specific to a particular installation, this file contains agent group definitions. Each line within the file defines a unique group of SNMP agents that *ForeView RMON **ST*** can access. To be included in this file, agent definitions must first be defined in the agent.lst file. Agent group names you specify can be up to 15 characters. You create and update this file through *ForeView RMON **ST***, although you can edit the file directly. You can define up to 100 agent groups in this file; each agent group can contain up to 60 agents.
- domain.lst. Available for use at any installation, this file contains domain definitions. Each line within the file defines a unique domain which represents a characterization of traffic. *ForeView RMON **ST*** supports two types of domains: Protocol and Generic. Protocol domains represent MAC, network and application layer protocols. Generic domains are part of the EnterpriseRMON specification, are available for use only on NETscout Probes, and are represented using a collection of filters. You create and update this file through *ForeView RMON **ST***'s Domain Editor application. Domain names you specify can be up to 8 characters. You can define up to 200 domains in this file.
- switch.def. Available for use at any installation, this file contains a list of switch vendors that *ForeView RMON **ST*** supports. Each line in the file defines a vendor-specific switch, as well as information about whether the switch contains any RMON support. Up to 100 switch types may be defined in this file. Do ***not*** edit this file, as it contains critical data. As additional switch types are supported in the future, FORE Systems will provide updated switch.def files.
- switch.lst. Specific to a particular installation, this file contains a list of defined switches you can use with *ForeView RMON **ST***. Each line within the file defines a unique switch. You create and update this file through *ForeView RMON **ST*** applications. Each agent in this file represents a switched SNMP agent that *ForeView RMON **ST*** can access. A switch is represented by all its ports, applicable attached dedicated agents, or roving agents. Switch names you specify can be up to 15 characters. To be included in this file, the switch type (vendor-specific) must first be defined in the switch.def file. You can define up to 1000 switches in this file.
- x.swp. Specific to a particular installation, this file contains a listing of port names, port numbers, interface numbers, slot numbers, interface types, and interface speeds for a specific switch. This file name is derived from the first 15 characters of the switch name. The number of lines in this file equals the number of discovered ports. Currently, *ForeView RMON **ST*** discovers only Ethernet and Fast Ethernet ports. *ForeView RMON **ST*** automatically creates this file when you use either the Learn function in *ForeView RMON **ST***, *ForeView RMON **ST*** (before you

launch Traffic Monitor for a defined switch), Domain Manager, or the dvlearn command line tool. To be included in this file, the switch must first be defined in the switch.lst file. Each switch listed in the switch.lst file must also have a corresponding x.swp file.

- x.frp. Specific to a particular installation, this file contains a listing of DLCI number, DLCI name, CIR definition, and virtual interface number for a specific frame relay agent. This file name is derived from the first 15 characters of the frame relay agent name. The number of lines in this file equals the number of discovered DLCI ports. *ForeView RMON **ST*** automatically creates this file, if it isn't already present before you launch Traffic Monitor for a frame relay agent, or when you use Domain Manager or the dvlearn command line tool. You can also create this file (except for the **vifn** field which contains the value of the virtual interface number) through either an ASCII text editor, such as vi, or build it incrementally by using the Edit Name feature in the Host List application. Using the Edit Name feature may be especially useful if a frame relay agent doesn't have the capability to automatically discover DLCIs.
- x.fil. Available for use at any installation, this file contains parameters set for a specific filter. This file name is derived from the first 15 characters of the filter name. The number of lines in this file depends upon the parameters you specify for the filter when you create it using the Filter Editor application. To edit an x.fil file, you can use either a text editor, or do so by editing a filter definition through the Filter Editor application. Each filter defined must also have a corresponding x.fil file. You can specify up to 200 filters in the *ForeView RMON **ST*** database.
- macaddr.nam. Specific to a particular installation, this file contains unique MAC address-to-name mapping information. Each line within the file contains a MAC address and the corresponding name you've defined for a host. You can create this file through either an ASCII text editor, such as vi, or build it incrementally by using the Edit Name feature in the Host List application. You can specify name mappings for up to 10,000 MAC addresses in this file.
- ipaddr.nam. Specific to a particular installation, this file contains unique IP address-to-name mapping information. Each line within the file contains an IP address and the corresponding name you've defined for a host. Although this file is typically a copy of the etc/hosts file, you could choose to build it incrementally by using the Edit Name feature in the Host List application. You can specify name mappings for up to 10,000 IP addresses in this file.
- vendorid.nam. Available for use at any installation, this file contains unique vendor ID to name mapping information. Each line within the file contains a vendor code and the corresponding vendor ID. Editing this file is not advised.
- vlan.nam. Specific to each application, this file contains unique VLAN (Virtual LAN) to name mapping information. Each line within the file contains a VLAN ID and the corresponding VLAN name you've defined. You can create this file

through either an ASCII text editor, such as vi, or build it incrementally by using the Edit Name feature in the Host List application. You can specify up to 500 VLAN IDs and names in this file.

- default.dvp. Available for use at any installation, this file contains unique agent/domain configuration parameters. Editing this file is not advised.
- domtree.inf. Available for use at any installation, this file contains parent-child relationship definitions between various domains. FORE Systems supplies this file as part of the *ForeView RMON **ST*** software. You can enhance and edit this file through any ASCII text editor, such as vi. The Protocol Monitor and Trend Reporter applications primarily use this file.
- x.mib. Available for use at any installation, this file contains variable names and corresponding object ID information. Each line within the file contains a variable name and the corresponding object ID (oid). This file name is derived from the first 15 characters of the MIB name. The number of lines in this file equals the number of variables in the MIB. FORE Systems ships several x.mib files with *ForeView RMON **ST***. Keep in mind that these files are created when we compile MIB/RFC with a standard MIB compiler; x.mib files do not contain comment lines or headers. This is an important distinction, because other configuration files that we create, or that are created automatically when you use an *ForeView RMON **ST*** application, do contain comment lines and headers.
- pvartrap.inf. Specific to a particular installation, this file contains definitions for MIB variables whose trap characteristics should be modified by Trap Manager. Each line within the file contains a variable name; trap numbers that indicate trap type, rising threshold, and falling threshold; and the sysoid.
- x.rtp. Specific to a particular installation, this file contains unique logical router name-to-interface number mapping. Each line within the file contains interface number and the corresponding name you've defined for the router. This file name is derived from the first 15 characters of the corresponding agent name. This file is built incrementally by using the Edit Name feature in the Host List application. You can specify interface-to-name mappings for up to 1000 routers in this file.
- applayer1.inf. Available for use at any installation, this file contains protocol name and ID information. Each line within the file contains a protocol name and the associated ID number. This file, used only in the Domain Editor application, specifies the available protocols you can select for application layer one. FORE Systems ships this file with *ForeView RMON **ST***. If necessary, you can edit this file using any ASCII text editor, such as vi.
- applayer2.inf. Available for use at any installation, this file contains protocol name and ID information. Each line within the file contains a protocol name and the associated ID number. This file, used only in the Domain Editor application,

specifies the available protocols you can select for application layer two. FORE Systems ships this file with *ForeView RMON **ST***. If necessary, you can edit this file using any ASCII text editor, such as vi.

- applayer3.inf. Available for use at any installation, this file contains protocol name and ID information. Each line within the file contains a protocol name and the associated ID number. This file, used only in the Domain Editor application, specifies the available protocols you can select for application layer three. FORE Systems ships this file with *ForeView RMON **ST***. If necessary, you can edit this file using any ASCII text editor, such as vi.
- applayer4.inf. Available for use at any installation, this file contains protocol name and ID information. Each line within the file contains a protocol name and the associated ID number. This file, used only in the Domain Editor application, specifies the available protocols you can select for application layer four. FORE Systems ships this file with *ForeView RMON **ST***. If necessary, you can edit this file using any ASCII text editor, such as vi.
- applyer5.inf. Available for use at any installation, this file contains protocol name and ID information. Each line within the file contains a protocol name and the associated ID number. This file, used only in the Domain Editor application, specifies the available protocols you can select for application layer five. FORE Systems ships this file with *ForeView RMON **ST***. If necessary, you can edit this file using any ASCII text editor, such as vi.
- dllayer.inf. Available for use at any installation, this file contains protocol name and ID information. Each line within the file contains a protocol name and the associated ID number. This file, used only in the Domain Editor application, specifies the available protocols you can select for the physical (data-link) layer. FORE Systems ships this file with *ForeView RMON **ST***. If necessary, you can edit this file using any ASCII text editor, such as vi.
- nllayer.inf. Available for use at any installation, this file contains protocol name and ID information. Each line within the file contains a protocol name and the associated ID number. This file, used only in the Domain Editor application, specifies the available protocols you can select for the network layer. FORE Systems ships this file with *ForeView RMON **ST***. If necessary, you can edit this file using any ASCII text editor, such as vi.

# APPENDIX B Error Messages

## B.1 *ForeView RMON ST* Error Messages

This appendix provides a list of the most commonly encountered *ForeView RMON **ST*** error messages.

`Error Message "Invalid Domain Name"`

**Explanation** This error usually occurs when running functions from the command line. It means the domain name used is not correct. You may also see this message in Domain Manager due to improper syntax of name.

`Error Message "Domain not present in Agent"`

**Explanation** This error usually occurs when running functions from the command line. This can be due to an incorrect domain name, or because the domain you specify has been deinstalled.

`Error Message "Invalid Agent Name"`

**Explanation** This error usually occurs when running functions from the command line. This can be due to an incorrect agent name, or because the agent has been deleted from *ForeView RMON **ST***.

`Error Message "Entry or Group not present in Agent"`

**Explanation** This error can occur if the domain you have specified has been deinstalled from the agent.

`Error Message "No Memory available"`

**Explanation** Not enough memory available to run the application.

`Error Message "Max Agents already in use"`

**Explanation** This error indicates that you have reached the maximum number of agents allowed in *ForeView RMON **ST***. The limits are 500 agents for the UNIX version.

```
Error Message   "No more resources in Agent"
```

**Explanation** This error indicates that the agent has run out of resources to handle the number of tasks you have specified. One example is that you can only do four simultaneous data captures outside Domains.

```
Error Message   "Cannot communicate with Agent"
```

**Explanation** The error indicates that the agent is not responding to *ForeView RMON **ST***. This error may indicate that the community string used by *ForeView RMON **ST*** is invalid. It can also be caused by a variety of physical or configuration problems at the agent.

```
Error Message   "Unexpected SNMPAPI error, See console window for
details"
```

**Explanation** This error can be due to a variety of causes. The console window provides additional information on the problem.

```
Error Message   "No resources in Agent, See console window for
details"
```

**Explanation** This error indicates that the agent has insufficient resources to handle a request. Additional details are presented in the console window.

# APPENDIX C Assigned Numbers

## C.1 Well-Known UDP and TCP ports

You can find a list of well-known UDP and TCP ports in the most recent "Assigned Numbers" RFC. The current Assigned Numbers RFC is RFC 1700 (10/20/94, 230 pages).

You can retrieve RFC 1700 (and other RFCs) using a Web browser at the URL:

`http://ds.internic.net/ds/dspglintdoc.html`

Or, using anonymous FTP, from:

`ds.internic.net, directory /rfc.`

# APPENDIX D NETscout Probe Applications

Three of the *ForeView RMON* ***ST*** applications were designed specifically for use with the NETscout Probe from Frontier Software. These three applications take advantage of proprietary MIBs to add functionality not provided by Standard RMON MIBs. The three applications are as follows:

- **Resource Monitor** - a tool that enables the use of proxy resources to lessen the demands placed on resources by RMON activities.
- **Protocol Monitor** - a tool that is useful in monitoring multiple sites in a network simultaneously.
- **Remote Login** - a tool used to configure the NETscout Probe. It is used to change parameters on the probe such as IP address and Gateway address, and to upgrade the software on the probe. Remote Login does not work for other third party probes.

The following sections contain more detailed information on Resource Monitor, Protocol Monitor, and Remote Login.

# D.1 Managing Remote Resources with Resource Monitor

Network administrators are increasingly using RMON probes to monitor LAN traffic because of the economic benefits that result from distributing management devices onto critical remote network segments —whether in a large corporate facility or across the country.

However, SNMP management creates problems due to the amount of bandwidth needed to get SNMP management information from a remote site. The dilemma for the administrator is that if network management bandwidth is minimized for SNMP polling and ping sweeps, then it's possible to miss network fault conditions, which could jeopardize the health of the enterprise network.

The ideal solution is to combine the use of domains and remote SNMP management (resource management) into a single, cost-effective device that can provide active management for all critical resources at the remote site, while also eliminating expensive and congestive regular polling. Integrating these two important network management technologies has resulted in *ForeView RMON **ST*** Resource Monitor.


Resource Monitor is available as an option on NETscout Probes, but isn't available on agents provided by other vendors.

Resource Monitor lets you efficiently monitor the resources of any SNMP device. To do so, the *ForeView RMON **ST*** console downloads MIB variables selected from a list to the agent, creating *proxy resources* at the agent (Figure D.1). Now, instead of polling from the management console, the agent polls each resource at a selected interval and records the result. You can select either an SNMP "get" or an IP ping resource.

In addition, you can set alarms in the agent and be notified when any variable reaches a predetermined value. In this way, the agent notifies the management console only when an alarm condition sets off a trap, eliminating continuous polling, as illustrated by Figure D.1 on Page D-3.

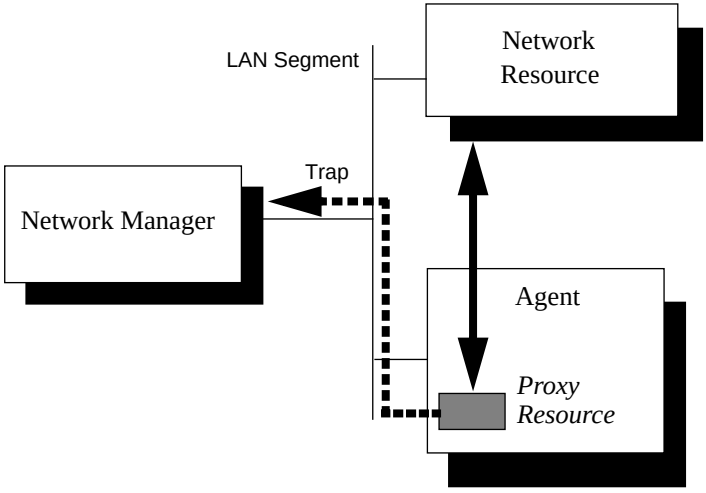



**Figure D.1 -** Using proxy resources to send traps to *ForeView RMON **ST***

## D.1.1 Resource Monitor Basics

In this chapter, the term “resource” means any SNMP-based network device. Such devices include routers, hosts, servers, and bridges, among others.

**NOTE** Resource monitor is an optional add-on for the NETscout Probe.

It’s useful to monitor network resources from a central point, especially if you want to be alerted when the network performs certain functions, or reaches specific utilization levels. For example, you may want to be alerted if a router’s utilization exceeds a certain point, if a host stops responding, or if a server’s disk space falls below a certain level.

However, remotely monitoring critical network resources has traditionally been difficult because polling the resource from the network manager occupies excessive bandwidth and ties up valuable network resources as illustrated by Figure D.2 on Page D-4. *ForeView RMON **ST***’s Resource Monitor uses proxy resources to solve this problem.

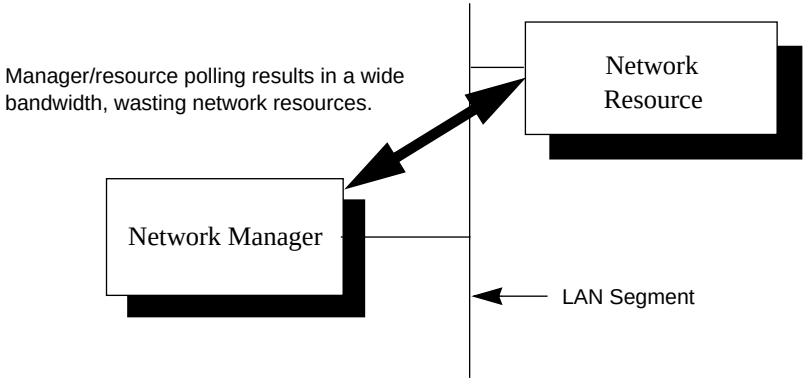



**Figure D.2 -** Network manager directly monitoring network resources

## D.1.2 How Resource Monitor Works

*ForeView RMON **ST***'s Resource Monitor lets you select and monitor network resources without consuming large amounts of network resources. Used with single-agent, single-domain situations, Resource Monitor combines both Domain View and remote SNMP management into one easy-to-use tool.

This tool lets you use proxy resources to actively manage all critical resources at a remote site, including private MIBs, which eliminate regular polling between a management station and an agent. The result is that the agent polls the resource, so that polling is limited to the segment and doesn't consume network resources.

Resource Monitor gives you two types of proxy resources to use. Depending on what you want to monitor, you'll choose from:

- **Proxy SNMP "get."** This proxy type identifies and collects data on a specific MIB variable on the resource (even if it's a private MIB). For example, you might want to specify a server's disk space MIB for monitoring and Trap Management, to be sure you're notified, if disk space exceeds a certain point.
- **Proxy IP Ping**. This proxy type pings a resource to ensure that it's alive on the network. You'll also want to use Trap Manager with this proxy type, as well.

### D.1.2.1 About Proxy Resources

The real key to Resource Monitor's flexibility and ease-of-use is how it uses proxy resources. You can assign a proxy SNMP "get" to any SNMP-based network device, such as a server, switch, or bridge, among others. When you do so, the NETscout probe attached to the network segment can collect specific data from the device. The NETscout probe stores the collected

data internally and *ForeView RMON **ST*** retrieves it when needed, as illustrated by Figure D.3. Typically, you'll want to use Trap Manager to set up threshold conditions for the data, so you're notified when the resource is in trouble.

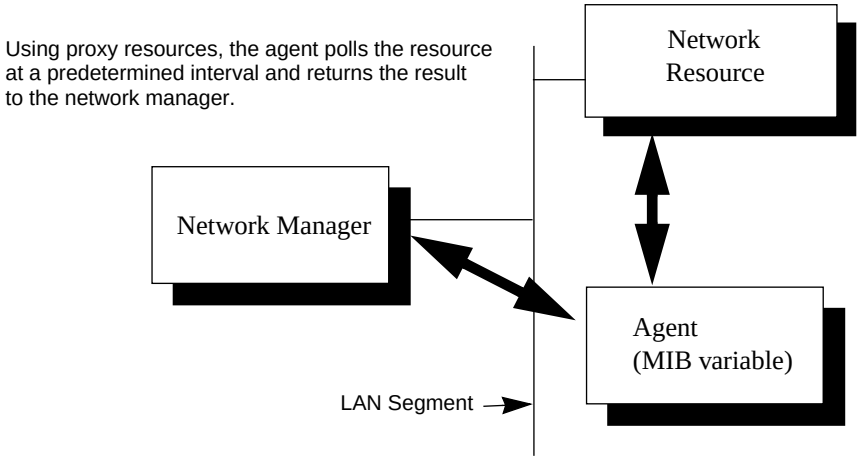



**Figure D.3 -** Using Resource Monitor to monitor network resources

For example, suppose you want to monitor available disk space on a server. First, use Resource Monitor to create a proxy SNMP "get" on the agent to read the MIB variable for server disk space. (This assumes that the MIB on the agent you use has a variable that reads this value.) Then select a host so that the agent knows which resource you're targeting. You now can use Trap Manager to create a trap to trigger an alarm when the disk space variable falls below a predetermined value.

The agent polls the resource at the interval you specified when you set up the proxy resource, and triggers an alarm when the disk space falls below the specified threshold.

When using the proxy IP Ping, you can specify that an agent pings a resource at certain intervals to ensure that it's alive on the segment. Using Trap Manager, you can specify that you're notified if the proxy ping can't be completed.

## D.1.3 Using Resource Monitor

It's easy to use Resource Monitor to install new proxy resources, or view or delete existing proxy resources at an agent. In this section are the procedures you'll use to work with Resource Monitor.

### D.1.3.1 Installing Proxy Resources on an Agent

There are two types of proxy resource: SNMP get and IP Ping. The resources that are displayed in the Resource Monitor list box, as well as the resources you add, view, or delete, reflect the type of resource you select. The default selection is SNMP. To use the Resource Monitor to install either type of proxy resource on a specific agent, use the following procedure.

1. Select the agent from the list box in the *ForeView RMON **ST*** main window and click on **Resource Monitor**. The SNMP Resource Monitor window is displayed as shown in Figure D.4. Note that the selected agent is displayed at the top of the window.

**Figure D.4 -** SNMP Resource Monitor Window

2. Select Type from the menu bar, and then click on either SNMP or IP Ping. If you select IP Ping, the IP Resource Monitor window is displayed as shown in Figure D.5 on Page D-7.

**Figure D.5 -** IP Resource Monitor window

### D.1.3.2 Understanding the Resource Monitor List Box Contents

The Resource Monitor list box contains several headings with values shown below. The list box you see depends on whether you selected Type/SNMP or Type/IP Ping from the menu bar. Table D.1 and Table  below explain the terms in the list boxes displayed by each selection.

**Table D.1 -** Resource Monitor List Box for SNMP Types

| This SNMP type heading: | Shows you: |
|---|---|
| Host | the name or IP address of the host associated with the resource. You must specify a host so the agent knows which network device you're targeting. |
| MIB | the name of the MIB associated with the SNMP proxy resource. |
| Variable.instance | the exact MIB variable that you want to monitor, such as free disk space on a server. Instance lets you index multiple occurrences of the same MIB variable. When MIB variables occur more than once, you must provide the instance you want to monitor. If there's only one instance of the variable, set instance to 1. |

**Table D.1 -** *(Continued)* Resource Monitor List Box for SNMP Types

| This SNMP type heading: | Shows you: |
|---|---|
| Value | the value of the last update of the variable being monitored. For example, if you're monitoring free disk space, Value is the amount of free space left. |
| Errors | the number of errors, if any, the agent finds when it polls the resource. If the agent finds errors, the value shown in the Value field may be inaccurate. |

**Table D.2 -** Resource Monitor List Box for IP Ping Types

| This IP Ping heading: | Shows you: |
|---|---|
| Host | the name or IP address of the host associated with the resource. You must specify a host so the agent knows which network device you're targeting. |
| Ping Interval | the number of seconds you specify between samples. The allowed range is a decimal integer from 1 to 3600 seconds. The default is 60 seconds. |
| Response Time (ms) | the amount of time, in milliseconds, that passed before the resource responded to the ping. |
| Errors | the number of errors that occurred when the agent tried to ping the resource. |

### D.1.3.3 Selecting the Sample Interval

You can select the time interval, which is how long the proxy resource waits before updating *ForeView RMON **ST***. The range is from 15 seconds to 5 minutes. The default is 1 minute. To select the sample interval, use the following procedure.

1. Select Sample from the menu bar.
2. Click on the sample interval you want.

### D.1.3.4 Adding an SNMP "get" Proxy Resource

You add an SNMP "get" proxy resource when you want to monitor a selected MIB variable on a network resource. The proxy resource returns the value of that variable at each polling interval, and any associated errors. To add a new SNMP "get" proxy resource at an agent, use the following procedure.

NOTE

You cannot add a proxy resource to an agent group. You can only add a proxy resource to a single agent or switch port.

1. Select the agent you want from the list box in the *ForeView RMON **ST*** window and click on **Resource Monitor**. The Resource Monitor window is displayed as shown in Figure D.4 on Page D-6. Note that the selected agent is displayed at the top of the window.
2. Select Type/SNMP from the menu bar.

All currently installed SNMP resources for the agent you selected are displayed in the list box.

3. Click on the Add button to display the Add SNMP Resource window shown in Figure D.6.

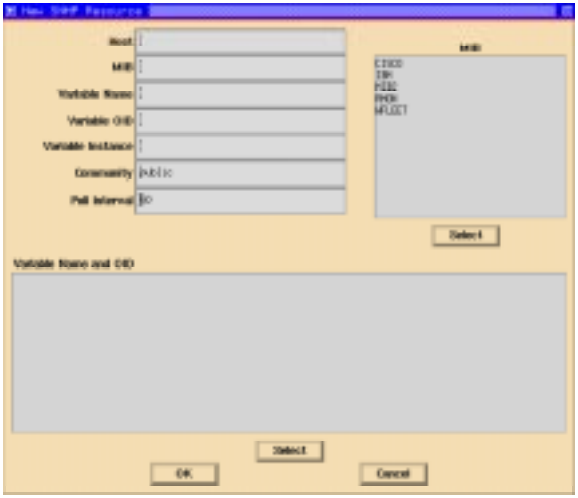


**Figure D.6 -** Add SNMP Resource window

4. In the **Host** field, enter the name or IP address of the host you want the agent to monitor.
5. The **MIB** list box displays a list of MIBs for the agent you selected. A MIB is a pre-defined database that determines the type of information an SNMP agent collects. Now do one of the following:
   - If the MIB you want **is not** displayed, go to Step 6.
     *or*

- If the MIB you want **is** displayed, highlight the appropriate MIB and select it by clicking on the Select button under the list box. Go to Step 7.

When you select a MIB, *ForeView RMON **ST*** fills in both the **Community** and the **Poll Interval** fields, as well as the **Variable Name and OID** list box. The table below explains these fields.

| This field: | Describes: |
|---|---|
| Community | a string identifier for the SNMP host you want to monitor. Set this field to the value for the host you want. The default value is **public**. |
| Poll Interval | the number of seconds you specify between samples. The allowed range is a decimal integer from 1 to 65535 seconds. The default is **60** seconds. |
| Variables | the various MIB variables that you can select and monitor with the new proxy resource. Keep in mind, though that the variable you select must be one with an integer value; text value variables cannot be evaluated and cause errors. Variables are specific to each MIB and are published with the MIB's information. Consult the MIB information manual to select the correct variable. The Variable OID is the Object Identifier for the object, defined by the variable's location in the SNMP MIB hierarchy. |

6. When the MIB you want to use for an SNMP device isn't shown in the MIB list box, just copy the MIB file you want into the $NSHOME/user directory. Once you do so, the filename is displayed in the MIB list box; now you can go back to Step 5.
7. Highlight the Variable Name and OID you want from the list box and click on the Select button beneath the list box to select it.
8. Enter the correct value in the **Variable Instance** field. The value must be a decimal number and must match the value given in your MIB data.
9. Click on OK to add the new proxy resource or Cancel to return to the Resource Monitor window.

*ForeView RMON **ST*** lists the new proxy resource in the list box on the Resource Monitor main window.

### D.1.3.5 Adding an IP Ping Resource

An IP Ping proxy resource pings the resource and tells you if it responds. When associated with a condition you set in Trap Manager, this provides an effective way of periodically checking critical network resources and receiving automatic notification if a resource goes down.

To add a new IP Ping proxy resource at an agent, use the following procedure.

1. Select the agent you want from the list box in the *ForeView RMON* ***ST*** window and click on **Resource Monitor**. The Resource Monitor window is displayed as shown in Figure D.4 on Page D-6. Note that the selected agent is displayed at the top of the window.
2. Select Type/IP Ping from the menu bar. All current IP Ping resources are displayed in the list box for the selected agent.
3. Click on the Add button to display the Add IP Ping Resource window. The IP Ping Resource window is displayed as shown in Figure D.7.

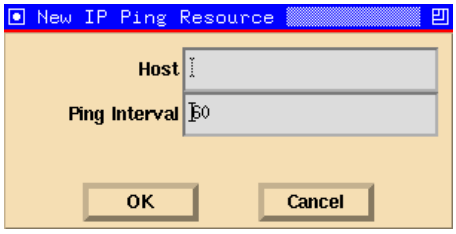



**Figure D.7 -** Add IP Ping Resource Window

4. In the Host field, enter either the IP address or the name of the host for this resource.
5. In the Ping Interval field, enter the number of seconds you want to use as an interval between pings. The range is a decimal integer from 1 to 3600, with a default of **60**.
6. Click on OK to install the new proxy resource, or Cancel to return to the Resource Monitor window. The resource is listed with the selected agent in the list box on the Resource Monitor window.

### D.1.3.6 Viewing a Proxy Resource

You may want to view a summary of all the values associated with a resource. This includes the values you enter when you define the proxy resource, and the values that are displayed for the resource in the Resource Monitor window. To view a resource in detail, use the following procedure.

1. Select the agent you want from the list box in the *ForeView RMON* ***ST*** window and click on **Resource Monitor**. The Resource Monitor window is displayed as shown in Figure D.4 on Page D-6. Note that the selected agent is displayed at the top of the window.

2. Select either Type/SNMP or Type/IP Ping from the menu bar, depending on the type of resource you want to see. All existing resources of that type you chose for the selected agent are displayed in the list box.
3. From the list box, select the resource you want to see in more detail.
4. When you click on View, one of the following occurs, depending on the type of resource you have selected:
   - **If you selected** Type/SNMP, the View SNMP Resource window is displayed as shown in Figure D.8.

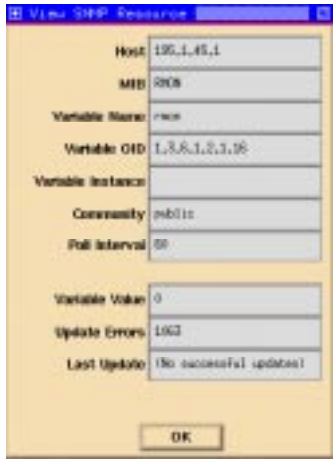



**Figure D.8 -** View SNMP Resource

   - **If you selected** Type/IP Ping, the View IP Ping Resource window is displayed as shown in Figure D.9.

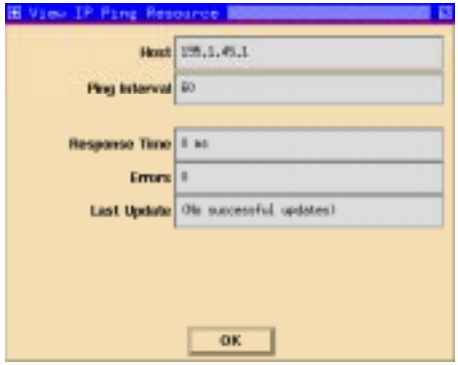



**Figure D.9 -** View IP Ping Resource

5. When you are finished viewing the information on the window, click on OK to return to the Resource Monitor window.

### D.1.3.7 Deleting a Proxy Resource

When you no longer need to poll a certain variable, it's a good idea to delete the proxy resource associated with it, to conserve agent resources. To delete a proxy resource, use the following procedure.

1. Select the agent you want from the list box in the *ForeView RMON **ST*** window and click on **Resource Monitor**. The Resource Monitor window is displayed as shown in Figure D.4 on Page D-6. Note that the selected agent is displayed at the top of the window.
2. Highlight the resource you want to delete in the list box in the Resource Monitor window.
3. Select Delete. A cautionary window is displayed, prompting you to confirm that you want to continue deleting the resource.
4. Select OK to delete the resource or Cancel to return to the Resource Monitor window.

## D.1.4 Getting Agent Information

Using Resource Monitor, you can directly see a description of the selected agent's system information (includes location, description, and how long the agent's been up and running, among others) and interface configuration (includes physical address, type, description, network speed, and status, among others). To view agent information, use the following procedure.

1. Select Tools/Agent Info from the menu bar.

The Agent Information window is displayed as shown in Figure D.10 on Page D-14.


**Figure D.10 -** Agent Information window

2. Click on OK when you're finished viewing the agent information.

### D.1.4.1 Printing Resource Monitor Data

You can print the data contained in the Resource Monitor window at any time. To do so, use the following procedure.

1. Select File/Print from the menu bar. The Print Options window shown in Figure D.11 is displayed.


**Figure D.11 -** Print Options window

2. Do one of the following:
   - To print data to a file, select File as the destination, specify the directory path under **Directory**, and type the filename in the **File** field.
     *or*
   - To print data directly to a printer, select Printer as the destination, and type the printer name in the **Printer** field.
3. Select Apply.

## D.1.5 Exiting Resource Monitor

To exit Resource Monitor at any time, just select File/Exit from the menu bar.

# D.2 Using Protocol Monitor

Protocol Monitor gives you an overview of network activity by converting raw network data gathered by agents and switches into easy-to-read graphical displays—displays you can transpose and invert to get two different views of the same data. This monitoring tool graphically displays network traffic statistics simultaneously for a number of selected agents, providing you with an at-a-glance comparison of multiple network segments.

Protocol Monitor is an excellent tool for monitoring or diagnosing your network. This application lets you monitor multiple sites simultaneously. It supports seven-layer protocol monitoring, letting you track protocol statistics at the network level. Monitoring the traffic on your network with Protocol Monitors gives you a fairly comprehensive picture of your network's operation.

You can use Protocol Monitor to establish a baseline of "normal" or expected performance and note any deviations from that performance that might signal broader network problems. You can then launch additional *ForeView RMON **ST*** tools to examine these suspect areas, or simply monitor certain aspects of your network in greater detail.

## D.2.1 Protocol Monitor

Protocol Monitor lets you monitor multiple sites by protocols. It lets you view selected statistics, such as utilization, byte rate, and packet rate in terms of the protocols that make up your network traffic. Using Protocol Monitor, you can see at a glance the protocol breakdown of your network's traffic and get a real-time picture of your network's operation.

Protocol Monitor also lets you "drill down" and view parent/child protocol relationships, to give you a more detailed view of just how specific protocols are being used on your network.

## D.2.2 Features of Protocol Monitor

The following features are available using Protocol Monitor. These features are common to both Protocol Monitor and Traffic Monitor. Implementation of these features is explained in Chapter 5: Monitoring the Network using Traffic Monitor.

### D.2.2.1 Display Properties

Protocol Monitor displays selected network information graphically. These displays give you an at-a-glance overview of your network. You will notice a Properties menu heading in each of their main windows. Under this heading, you can choose to display selected network data as a 2-D bar graph, a 3-D bar graph or a 3-D pie chart. In addition to these three graphical display choices, you can also transpose or invert the displays.

### D.2.2.2 Transposing Displays

This powerful feature lets you transpose both bar graph and pie chart displays to get two different views of the same data. In the default display of Protocol Monitor, the statistics you select are displayed as functions of different agents. But when you choose to transpose the bar-graph or pie-chart display, the agents are displayed as functions of the statistics.

### D.2.2.3 Inverting Displays

You can choose to view a bar graph in inverted form. This inverts the axes of the two bar graph displays (2-D and 3-D). You may choose to switch the x and y axes as a matter of viewing preference depending on the data you're displaying. Sometimes when you manipulate and resize a bar graph window, inverting the graph provides a clearer picture of the data and devices you are monitoring.

### D.2.2.4 Manipulating 3-D Graphs

In any 3-D graph, such as a bar graph or pie chart, you can manipulate the elevation, depth, and angle of the displayed graph directly with the mouse. This lets you increase or decrease the three-dimensional effect of the graph according to your preference.

Use the following procedure to manipulate the displayed 3-D graph with your mouse.

1. Move the cursor over the three-dimensional graph you want to manipulate.
2. Do one of the following:
   - If you have a three button mouse, press and hold down the middle mouse button.
     *or*
   - If you have a two button mouse, simultaneously press both mouse buttons and hold them down.
3. Drag the cursor to manipulate the graph. When the graphic is positioned the way you want it, release any mouse buttons you've pressed.

#### D.2.2.4.1 Resetting Graphs

Use the following procedure to reset any graph you've manipulated back to the original positions.

1. On the graph you want to reset, put the cursor anywhere in the graph.
2. To restore the original positioning of the graph, type the following:

**+**

#### D.2.2.4.2 Printing the Display

You can print any bar graph or pie chart you're viewing in the Protocol monitor to either a printer or a file. To print the display, make sure the window containing the bar graph or pie chart you want to print is current, and use the following procedure.

1. To open the Print Options dialog box, select File/Print from the menu bar. Figure D.12 shows the Print Options dialog box.


**Figure D.12 -** Print Options window

2. Do one of the following:
   - To print the graph to a file, select File as the destination, specify the directory path under **Directory**, and type the filename in the **File** field.
     *or*
   - To print the graph directly to a printer, select Printer as the destination, and type the printer name in the **Printer** field.
3. Click on Apply.

### D.2.2.5 Changing the Sample Rate

In Protocol monitor, you are monitoring samples collected by network agents or switches you have added to the *ForeView RMON **ST*** client software. When you choose to monitor selected data, *ForeView RMON **ST*** polls the agents or switches you select at intervals you specify and updates the display. You can change this interval in either the Traffic or Protocol monitor by selecting the Sample menu from application's menu bar and selecting the sample rate you want.

### D.2.2.6 Launching Additional *ForeView RMON ST* Tools for a Closer Look

As mentioned earlier, Protocol Monitor is one of *ForeView RMON* ***ST***'s general monitoring tools. It gives you an excellent overview of your network, based on the data you choose to monitor. But there may be times when you want to take a closer look at a particular aspect of your network for more detailed monitoring or network diagnosis.

To do so, you can launch additional tools available under the Tools menu. Tools such as Segment Statistics let you zoom in on aspects of your network and the data flowing through it for a more detailed analysis. See Chapter 7: Monitoring and Troubleshooting Single Domains for information about these and about additional *ForeView RMON* ***ST*** tools.

### D.2.2.7 Operating Independent Displays

The *ForeView RMON* ***ST*** console is actually an applications suite where you can launch multiple *ForeView RMON* ***ST*** software applications. You can bring up several windows of the same *ForeView RMON* ***ST*** application. For example, although Protocol Monitor lets you monitor several types of data, you can only monitor one type of data at a time. You can, however, bring up several different Protocol Monitor windows and select different data types to monitor for each; Protocol Monitor displays operate independently of the other. Remember, however, that each window you open uses additional *ForeView RMON* ***ST*** resources.

## D.3 Monitoring Remote Sites Using Protocol Monitor

In this section, you'll learn how to start and use Protocol Monitor to monitor your network in terms of its protocol composition. The following discussion steps you through each procedure and includes a detailed explanation of every available option and feature.



## D.3.1 Displaying Protocol Monitor

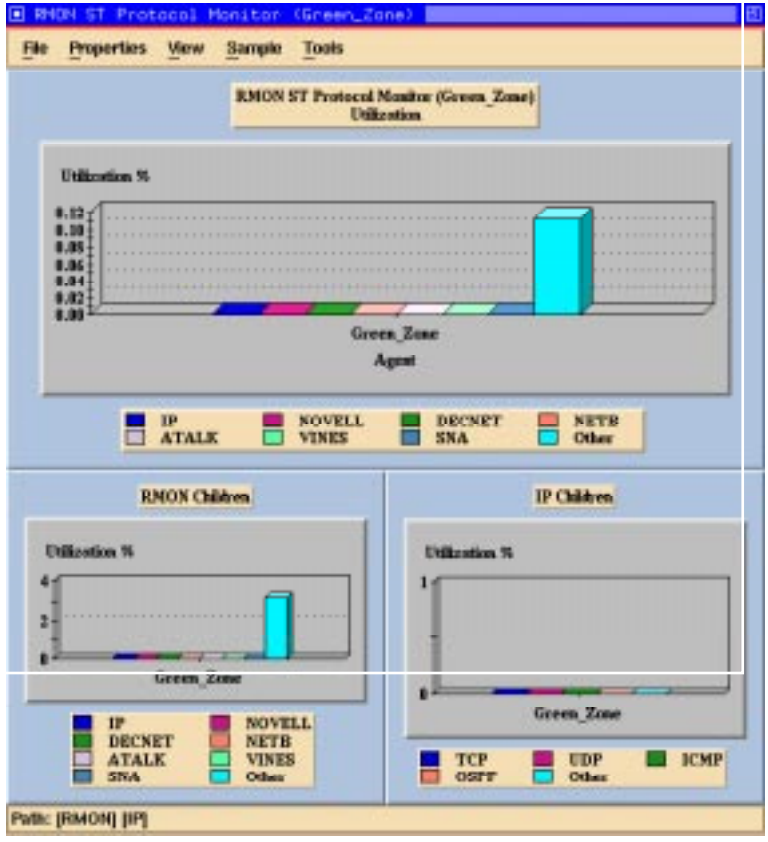
Use the following procedure to display Protocol Monitor from the *ForeView RMON* ***ST*** main window. After you display the Protocol Monitor application, you can begin to monitor your network's traffic in terms of protocol information.

1. Log in to the network management station where *ForeView RMON* ***ST*** is installed, and run the *ForeView RMON* ***ST*** application.
2. Select an agent, agent group, or switch from those shown in the list boxes in the *ForeView RMON* ***ST*** main window and click on the Protocol Monitor icon or select Application/Protocol Monitor from the menu bar.

NOTE

If the agent, group, or switch you want isn't listed, you may need to add it. To do so, see Chapter 4.

On the Protocol Monitor main window, you'll see three displays with one bar graph cluster or pie chart for each agent or agent group as shown in Figure D.13.




*Network layer area*

***Protocol*** ***<Protocol type> children***

**Figure D.13 -** Protocol Monitor main window

3. From this main window, you can begin to monitor your network in terms of protocol makeup and behavior, using various procedures described in this chapter.

## D.3.2 The Protocol Monitor Display

The Protocol Monitor display consists of three separate-but-related displays, as shown in Figure D.13. The display shows:

- **Network layer area**. This area shows the selected statistic in terms of network layer protocols.
- **Protocol area**. This area displays the selected statistic in terms of the high-level protocols that have children protocols.
- **<Protocol type> children area**. Shows the selected statistic in terms of the children of a particular protocol.


The domain designated "Other" in the legend of each graphic display refers to the segment traffic that remains when all other listed domains are subtracted from the total segment traffic.

### D.3.2.1 Viewing Protocol Relationships

To give you a more detailed analysis of how your network is utilizing specific protocols, Protocol Monitor lets you "drill down" from the network layer protocols and view parent protocols and their respective children.

To view the children of a specific parent protocol, click on the corresponding color box in the Parents' legend. The children of that particular protocol are then displayed in the <*Protocol type*> *children* display area as shown in Figure D.13 on Page D-20.

#### D.3.2.1.1 Defining Protocol Parents and Children

You will only see the children of a particular parent protocol if the relationship has been defined in the text file $NSHOME/usr/domtree.inf. *ForeView RMON **ST*** comes with a number of protocol parent/child relationships already defined in this file, but in rare cases, you may want to redefine or add new parent/child relationships to better suit your network monitoring needs. An example of this configuration file is shown in Figure D.14 on Page D-22.

```
#
# Protocol parent-children relationship (File: domtree.inf)
#
RMON:           IP NOVELL DECNET ATALK VINES SNA
NOVELL:         NCP
IP:             TCP UDP ICMP
TCP:            FTP XWINDOW HTTP
UDP             SNMP NFS
```

**Figure D.14 -** domtree.inf configuration file example

## D.3.3 Viewing Network Statistics in Terms of Protocol

You can now select the type of data you want to monitor, the type of display, and the sample interval. Remember, although you can only monitor one data type at a time, you can simultaneously launch a number of Protocol Monitor windows, each monitoring a different statistic independent of the other windows.

## D.3.4 Graphical Display Choices

To select the type of graphical display you want to view the data, select the Properties menu and then the type of display. You have three graphical display choices:

- 2-D bar chart
- 3-D bar chart
- Pie chart

### D.3.4.1 Transposing and Inverting the Display

To either transpose or invert the display, do one of the following:

- To transpose the display as described in Transposing Displays on page 5-17, select Properties/Transpose from the menu bar.
- To invert a bar graph display as described in Inverting Displays on page 5-17, select Properties/Invert from the menu bar.

## D.3.5 Selecting the Data Type

You can now choose the type of data that you want to monitor by selecting the View menu and then selecting the data type. You have a choice of three data types:

- **Utilization** - The average percentage of bandwidth utilization on the network during the sample interval.
- **Byte Rate** - The number of kbytes / second in the selected interval.
- **Packet Rate** - The number of packets / second in the selected interval.

## D.3.6 Changing the Sample Rate

The sample rate is the interval of time that *ForeView RMON **ST*** waits before polling and updating the information displayed in the list box. You can change this sample rate to meet your needs, as shown below.

- 15 seconds
- 30 seconds
- 1 minute (default rate)
- 2 minutes
- 5 minutes

To change the sample rate, select Sample and then select one of the rates described above. *ForeView RMON **ST*** immediately uses the new sample rate to poll the segment and then update the information in the graphical display.

## D.3.7 Launching Tools from Protocol Monitor Graphs

You can launch single agent / domain tools from Protocol Monitor graphs. To do so, use the following procedure.

1. Select Tools from the menu bar, and click on the tool you want to launch.
2. If you selected an agent/domain combination, the Launch Application (Protocol Monitor) window is displayed as shown in Figure D.15 on Page D-24.

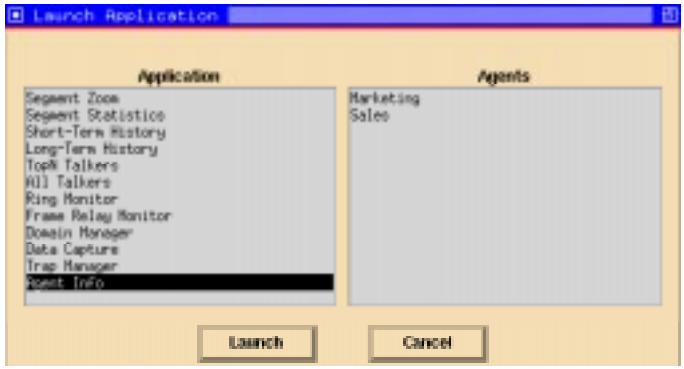



**Figure D.15 -** Launch Application window

3. Highlight the following:
   - Application you want to use
   - Agent you want to select
   - Domain you want to view
4. Click on Launch.

## D.3.8 Launching other Applications from Protocol Monitor

You can launch other segment and domain monitoring tools directly from Protocol Monitor. To do so, first select Tools and then any of the following:

- **Segment Statistics**. Launches the Segment Statistics tool, which displays four data views for the selected segment. See Chapter 7: Monitoring and Troubleshooting Single Domains for details.
- **Short-Term History**. Launches the Short-Term History graph, which displays short-term data (residing in the selected agent) for the period you select. See Chapter 7: Monitoring and Troubleshooting Single Domains for details.
- **Long-Term History**. Launches the Long-Term History graph, which displays long-term data (residing in the selected agent) for the period you select. See Chapter 7: Monitoring and Troubleshooting Single Domains for details.
- **Top N Talkers**. Launches the Top N Talkers graph, which displays the N numbers of hosts who are talking the most on the selected segment. See Chapter 7: Monitoring and Troubleshooting Single Domains for details.
- **Data Capture.** Launches Data Capture to capture selected data for later examination with Protocol Decode. See Chapter 11: Decoding Captured Packets with Protocol Decode for details.
- **Trap Manager.** Launches Trap Manager, which lets you monitor data thresholds by setting traps. See Chapter 8: Setting Alarms Using Trap Manager for details.
- **Agent Info**. Launches the Launch Application window that lets you select the agent you want information for. See Getting Agent Information on page 5-11 for details.

## D.3.9 Exiting Protocol Monitor

To exit Protocol Monitor, select File/Exit from the menu bar.

## D.4 Remote Login

Remote Login is the application that is used to configure Frontier Software's NETscout Probe network probes. Every NETscout Probe is configured according to a number of parameters such as IP address, and read / write community strings. If you have a NETscout Probe, you may want to change these parameters at certain agents as your network management needs change.

**CAUTION**

You can configure **only** Frontier NETscout Probes with Remote Login. This application will not work with network probes from other vendors.

The traditional problem in reconfiguring agents has been that agents may be physically located all over the world. *ForeView RMON **ST***'s Remote Login tool solves this problem by letting you configure agents directly from *ForeView RMON **ST*** through the network, regardless of where they are located. To configure an agent using Remote Login, use the following procedure.

1. Select the agent you want to reconfigure from the **Agents [All]** list box on the *ForeView RMON **ST*** main window.
2. Click on Remote Login from the *ForeView RMON **ST*** main window. The Remote Login window you'll see should be similar to the one shown below in Figure D.16.


**Figure D.16 -** Remote Login window

3. See the *NETscout Probe User Guide* for configuration instructions.
4. Change agent parameters according to the instructions in the agent manual. To change a parameter, enter the parameter number in the selection field at the bottom of the window, then modify the parameter.
5. To make your changes at the agent, enter the number for the **Reset Agent** choice.
6. To exit Remote Login, type exit in the selection field and press <Enter>.

# Index

**D**

**E**

**F**

**G**



**H**

**M**

**S**

**T**